Emerging Radio and MANET Technology Study

Research Support for a Survey of State-of-the-art Commercial and Military Hardware/Software for Mobile Ad hoc Networks

Glen Henderson
William Pase
Bell Canada

Prepared By:
Bell Canada
160 Elgin Street
17th floor
Ottawa, Ontario
K2P 2C4
Contract Project Manager: Darcy Simmelink, 613-998-1451
PWGSC Contract Number: W7714-08FE01
CSA: Dr. David Brown, 613-993-9963; Mazda Salmanian, 613-998-0649

Defence R&D Canada – Ottawa

Contract Report
DRDC-RDDC-2014-C208
October 2014

Abstract

This paper documents the results of a study into the architectural options for a situational awareness and command and control (SA+C2) device that could be used by tactical units. This device would connect individual unit members through a mobile ad-hoc network (MANET) based mesh topology to relay tactical information in a secure and robust manner while retaining the mobility needed for dismounted soldier operations. This study presents six architectural options for the proposed device each of which includes a graphical display and radio communications component. The currently available commercial off the shelf (COTS), military off the shelf (MOTS) and open source technologies in the areas of tablet devices, Wi-Fi network devices and broad spectrum radios are evaluated in the context of the proposed architectures. Of specific interest is the degree to which these components can be modified at a device or firmware level to support the development of additional situational awareness applications in support of tactical missions. The benefits and limitations of fully open architectures available through the open source community as compared with the closed architectures of vendor based products are discussed. Based on the interpretation of the information gathered, a recommended SA+C2 device hardware and software configuration is provided. Additionally, extensions to the architecture that would support enhancements to the baseline SA+C2 capability are proposed.

Executive summary

Emerging Radio and MANET Technology Study: Research Support for a Survey of State-of-the-art Commercial and Military Hardware/Software for Mobile Ad hoc Networks

Glen Henderson; William Pase; DRDC Ottawa CR [enter number only: 9999-999]; Defence R&D Canada – Ottawa; July 2014.

Introduction or background: The Cyber Operations and Signals Warfare section of Defence Research and Development Canada has an interest in technological and operational challenges in the cyber and physical battle spaces. One such challenge is to provide an integrated information/communication system and associated mobile devices for hosting command and control applications and linking situational awareness information between devices. Devices so configured and connected will allow dismounted soldiers to operate autonomously within a self-contained, secure networking environment.

This study is primarily directed towards mobile ad hoc networking (MANET) technologies due to their inherent flexibility. The needs of the individual dismounted soldier for mobility combined with the overarching need of the unit as a whole for reliable communications makes the MANET architecture well suited for a tactical deployment. In part, this study performs an options analysis with respect to potential architectures for a mobile situational awareness and command and control (SA+C2) device which consists of a graphical display, a communications component and the ability to link these components together for bi-directional information exchange.

Results: This study has documented six potential SA+C2 device architectures based on commercial off the shelf (COTS), military off the shelf (MOTS) and open source technologies. These architectures are primarily differentiated by the component that serves as the radio transmission device and the component that establishes the connection to the MANET. These architectures are defined as follows.

1. A tablet-based device where the integrated tablet radio is used to connect the MANET though software resident on the tablet itself.

2. An assisted architecture where the tablet-based radio broadcast range is enhanced with an external antenna.

3. An assisted architecture where the tablet-based radio’s capabilities are enhanced with an external wireless router.

4. An external radio architecture where the tablet leverages an external 802.11 radio while the tablet retains responsibility for participation in the MANET.

5. An external radio architecture where the tablet leverages an external full spectrum radio while the tablet retains responsibility for participation in the MANET.

6. A MOTS/COTS solution where a commercial radio product establishes and maintains the MANET and the graphical component access the MANET via the radio.

This investigation has made the following observations about the state of commercial and open source-based radio technologies.

- Programmable interfaces for most COTS/MOTS radio solutions do exist but are generally not made publicly available to the community. Vendors restrict access to these interfaces to their development team and solution partners. These interfaces may be shared to a wider community but only through a formalized relationship, such as a non-disclosure agreement.
- Conversely, the open source community is actively (and increasingly) involved in the creation of radio-based technologies. It is possible to obtain source code, architectural specifications and device drivers for radio products and extend the capabilities of those products through code modifications.
- Per unit cost differential between COTS/MOTS integrated solutions and the equivalent device created through commercial components is an order of magnitude higher. In a development lab context, a $5,000 military grade radio can be replaced with a $500 open source equivalent.
- Emerging capabilities for radio based devices are quickly released through the open source community although the degree of technical support is less formalized and requires in-depth knowledge on the part of the solution development team.
- Low cost, fully functional broad spectrum radios are becoming easily obtainable through online sources. These tools are of great interest to the radio hobbyist community and it is in the best interest of DRDC to examine the potential threats posed by these new devices.
- Full spectrum radios using low power components are currently not capable of processing 802.11 protocols at speed and are therefore not capable of serving as the networking device that will connect to the MANET.

Significance: Given the openness of the architecture, the ease of modification and the low per unit cost, the architectural option that best meets the device based communications needs for creating, using and manipulating MANETs is a tablet device with an external open architecture Wi-Fi radio.

While integrated COTS/MOTS solutions are more in line with traditional DND procurement practices, it is significant to note that the hardware and software provided through the open source community is more accessible to the general public. The recent trend towards the asymmetric threat (e.g., IEDs) demonstrates that there is tremendous value in knowing the capabilities of devices that can be easily procured and built using ubiquitously available technical information. With the goal of creating new tactical applications, DND will benefit from knowing the kind of threat that could be posed by the malicious participants in the developer community.

Given a goal of developing new on-the-move applications leveraging customizations to the device hardware and software, the accessibility of solutions that are based on open source technology is most in accord with the needs of this initiative. It is possible to combine multiple

solution elements beyond the deployment of MANET-capable devices and MANET-based applications to achieve a broader based SA+C2 device capability that provides a more complete solution for the tactical problem space. The basic device which includes SA and C2 applications that are enhanced by access to low-level device driver and firmware updates to the device components could be further enhanced by including a full spectrum radio and software to perform sensor data collection activities.

Future plans: Based on the results of this study, it is recommended that the investigation into an SA+C2 device be continued to further extend knowledge of the proposed platform. The following areas are recommended for continued investigation:

1. Evaluate existing COTS/MOTS software and hardware platforms on which a research lab could be based.

2. Perform a detailed options analysis for the formal specification of the hardware/software selection and configuration that will be used to construct and manage a high-bandwidth MANET for dismounted soldiers based on the recommended architecture in this report.

3. Deliver a functioning mobile ad-hoc network solution that supports multi-hop routing and self-configuration to support DRDC's ongoing work in this area.

4. Develop applications for the display device that utilize the MANET as a communications medium.

Table of contents

Abstract …….. i
Executive summary ii
Table of contents v
List of figures vii
List of tables viii
1 Introduction 1
1.1 Summary of the Solution Space 3
1.2 Document Structure 6
2 Architectural Specifications 7
2.1 Architectural Approaches 7
2.1.1 Tablet Only 7
2.1.2 Externally Assisted Tablet-based Communications 9
2.1.3 Networked Tablet and with External Radio 12
2.1.4 Tablet with Networked Radio 14
2.2 Summary of Representative Technologies 15
3 Analysis of Current Technologies 18
3.1 Radio Component 18
3.1.1 Military Grade Radios 19
3.1.1.1 TrellisWare Technologies 19
3.1.1.2 Persistent Systems 23
3.1.1.3 Harris Tactical Communications 27
3.1.1.4 Thales Group 29
3.1.1.5 SELEX ES 33
3.1.1.6 Other Notable Technology Providers 34
3.1.2 Commercial Radios 36
3.1.2.1 Tethered Solutions 37
3.1.2.2 Tablet Integrated Solutions 46
3.1.3 Open Source Radios 48
3.1.3.1 Great Scott Gadgets HackRF 48
3.1.3.2 Nuand bladeRF 50
3.1.3.3 ETTUS USRP B200/B210 51
3.1.3.4 RTL-SDR DVB-T 52
3.1.3.5 Additional Open Source Radios 53
3.1.3.6 Comparing Open Source Radios 54
3.1.4 Open Source SDR Support 55
3.1.4.1 GNU Radio 55
3.1.4.2 Kali Linux 57

3.2 Tablet Component 58
3.2.1 Tablet Configurations 58
3.2.2 Tablets and Radio Configuration 58
3.2.2.1 Internal Radios 59
3.2.2.2 External Radios 59
3.2.2.3 MANET Support for Radios 60
3.3 MANET Implementation 61
3.3.1 Tablet-based MANET Configuration 61
3.3.2 Radio-based MANET Configuration 63
3.3.2.1 TrellisWare Technologies 64
3.3.2.2 Persistent Systems 64
4 Interpretation of Results 66
4.1 Architectural Options Revisited 66
4.1.1 Option 1: Fully Open Hardware/Software Device Configuration 67
4.1.2 Option 2: Device Configuration Based on Commercial Offering 68
4.1.3 Summary of Options 69
4.2 Extending the Capability of the SA+C2 Device 71
4.2.1 Co-Existence and Isolation of Code on Android Devices 72
4.2.2 Security Enhanced Android 74
5 Summary and Recommendations 75
5.1 Future Work 77
References 78
List of symbols/abbreviations/acronyms/initialisms 79

List of figures

Figure 1: Baseline SA+C2 Device Architecture 4
Figure 2: Architecture 1: Tablet Only Architecture 8
Figure 3: Architecture 2a: Tablet with External Antenna 9
Figure 4: External Antenna Hardware Modifications 10
Figure 5: A Tablet with a Long Range Directional Antenna 10
Figure 6: Architecture 2b: Tablet with External Router 11
Figure 7: Architecture 3a: Tablet with External Wi-Fi Radio 12
Figure 8: Architecture 3b: Tablet with External Full Spectrum Radio 13
Figure 9: Architecture 4: Tablet with MANET-enabled Radio 14
Figure 10: Review of Architecture Types 17
Figure 11: Available Radio Components 18
Figure 12:Thales Cougar Team Networking Structure 30
Figure 13:St@rmille Device Networking 32
Figure 14: A Tablet-Based MANET 61
Figure 15: A Radio-Based MANET 64
Figure 16: Google Nexus 7 and External TP-link Wi-Fi Radio 68
Figure 18: Heterogeneous SA+C2 Device Deployments 72
Figure 19: A Software Jail 73
Figure 20: The Proposed SA+C2 Logical Architecture 76

List of tables

Table 1: Classification of SA+C2 Device Architectures 15
Table 2: Summary of Architectural Approaches 17
Table 3: TrellisWare CheetahNet TW-220 Specifications 20
Table 4: TrellisWare CUB TW-400 Specifications 21
Table 5: TrellisWare WildCat II TW-130 21
Table 6: Persistent Systems Android Kit 23
Table 7:Persistent Systems MPU GEN4 Specifications 24
Table 8: Persistent Systems Quad Radio Router 25
Table 9: Harris RF-7800S-TR Specifications 27
Table 10: Harris AN/PRC-152A Specifications 28
Table 11: Thales Cougar Team Specifications 29
Table 12: Thales St@r Mille Radio Specifications 31
Table 13: Selex ES Soldier System Radio 33
Table 14:USB Wi-Fi Device Information 38
Table 15: USB Wi-Fi Devices 39
Table 16: External Antenna Information 41
Table 17: Portable Routers 42
Table 18: Mini PC Manufacturer 44
Table 19: Raspberry Pi Information 45
Table 20: Android Tablet Information 47
Table 21: HackRF Specifications 48
Table 22:bladeRF Specifications 50
Table 23: Ettus radio Specifications 51
Table 24: RL-SDR DVB-T Specifications 52
Table 25: RTL2823U Chipsets and Associated Frequency Ranges 52
Table 26: GNURadio Reference Documentation Set 56
Table 27: KALI Linux Reference Documentation Set 57
Table 28: MANET Software for Android Devices 62
Table 29: Ad-hoc Networking and MANET Reference Documentation Set 63
Table 30: SA+C2 Device using Tablet and External Wi-Fi Radio 68

Table 31: A Comparison of SA+C2 Device Options 69

1 Introduction

The Cyber Operations and Signals Warfare (COSW) section of Defence Research and Development Canada (DRDC) has an interest in the technological and operational challenges in the cyber and physical battle spaces.

One such challenge is to provide an integrated information/communication system and associated mobile devices for hosting command and control (C2) applications and linking situational awareness (SA) information between devices. Devices in such a system, herein after referred to as mobile “SA+C2 devices”, will allow dismounted soldiers to operate autonomously within a self-contained, secure networking environment where each soldier’s handset includes:

- A communications component such as a broad spectrum radio or 802.11 transmitting device;
- A touch-based/graphical handheld device that can host applications used by soldiers in the field (e.g., blue force tracking);
- A means by which these two components can be connected.

This report documents the results of an investigation into current and emerging technologies that can connect handheld devices in a mesh or ad-hoc architecture without dependence on a pre-existing networking infrastructure. The intent of this effort is to investigate currently available commercial off the shelf (COTS) or military off the shelf (MOTS) components that can be combined to meet the configuration defined above. The scope of this investigation includes:

- A survey of known commercial offerings in radio technologies to determine:
    - The specifications of representative radio sets for operational performance (e.g., power consumption, range, frequency ranges);
    - The existence and accessibility of programmatic interfaces for COTS/MOTS radios;
    - The potential for altering the radio’s internal logic, signal processing or networking protocols;
    - The degree to which built-in mesh networking / ad-hoc networks can be supported from the radio technologies;
- A survey of COTS tablet technologies to determine:
    - The limitations of integrated radios, that is, radios that are engineered into the tablet design;

    - The ease by which an external communications component can be physically and logically connected to the tablet and accessed by higher order layers of the tablet operating system;

    - Any relevant implications to the management of ad-hoc networks by the tablet;

- A summary of the known methods by which tablets and external communication equipment can be physically connected and/or logically bound.

While it is possible to acquire and provision existing COTS handsets with integrated displays, these solutions have closed architectures and typically do not support:

- An externally accessible programmatic interface; or

- A method by which existing firmware-based technologies can be updated by third parties to introduce new or modified capabilities.

The need to equip dismounted soldiers with On-The-Move (OTM) capability has been recognized and prior projects that have studied this problem space have identified challenges in deploying these tools. An in-field experiment conducted by the U.S. Army Research Laboratory (US-ARL), Human Research and Engineering Directorate, concluded that networks comprised of dismounted soldiers and unmanned sensors did give command personnel better awareness of the position and mobility of dismounted troops. However, the solution was also observed to have:

1. Caused command personnel to become so involved with the interface other important tasks were neglected; and

2. Placed a burden on units in the form of additional physical and cognitive demands.

The US-ARL recommended continued efforts to develop robust communication networks and tactics, techniques, and procedures (TTPs) for coordinating these systems into the dismounted force [1]. The DRDC COSW section is addressing this challenge with the vision of developing new OTM applications that leverage the capabilities of the technology to improve SA and C2 functions.

Specifically, the SA+C2 device envisaged by COSW will foster the development of applications to address the challenges faced by solders in the field in terms of battle space comprehension: delivering information as it is needed, prioritizing information in context for the individual team member and ensuring that information is relayed in a clear and concise manner. The SA+C2 device will integrate with the soldier's space both physically and operationally so as to obtain the full benefit of SA information with the least amount of disruption to other tasks. This device then becomes an extension of the capabilities delivered by mobile ad hoc network (MANET) technologies: the ability to retain mobility in an information rich, low infrastructure networked environment.

To meet the hardware/software development objectives of the COSW section, this investigation focused on those components, architectures and methodologies that would enable the creation and deployment of new OTM applications; greater focus was placed on:

- Radios with programmable interfaces;
- Software Defined Radio (SDR) technologies;
- Open source projects and open architecture devices; and
- Devices with programmable kernels or where device modules could be integrated into the operation of the device.

The results presented in this report are based on interviews with representatives from the field of radio design and manufacturing as well as individuals with knowledge of the requirements of the soldier in theater. These results are also based on reviews of product specifications, analysis of technical papers related to SDR software/hardware and journals from community-based radio technology projects.

1.1 Summary of the Solution Space

The final vision for this solution is to equip dismounted soldiers with the technologies that will allow them to access C2 communication as well as perform SA information exchange while retaining mobility and being independent of any existing infrastructure. This means that the combined devices (radio and tablet) must be able to join in an infrastructure-less network environment. Such networks exist in many forms [2] including:

1. *Fully connected mesh networks*: A mesh network whose nodes are all connected to each other.

2. *Partially connected mesh networks*: A mesh network where each node is connected to one or more nodes and messages are relayed to destinations through routing protocols. When using a routing technique, the message is propagated along a path, by hopping from node to node until the destination is reached.

3. *Ad-hoc networks*: A form of partially connected mesh network where nodes can join and leave mesh (fluid participation). The routing protocols must allow for continuous connections and reconfiguration around broken or blocked paths, using self-healing algorithms.

4. *Mobile Ad-hoc Networks (MANETs)*: An ad-hoc network where the mobility/physical location of the individual nodes is a significant factor in the articulation of the mesh architecture. Nodes that become physically separate from the mesh can be disconnected from the network and, if they are playing an essential routing role, sever other nodes from the network as well.

This study is primarily directed towards MANET technologies due to their inherent flexibility. The needs of the individual dismounted soldier for mobility combined with the overarching need of the unit as a whole for reliable communications makes the MANET architecture best suited for a tactical deployment.

In part, this study performs an options analysis with respect to potential architectures for a mobile SA+C2 device. At the highest level, this device will include the following elements and information flows, as shown in Figure 1: *Baseline SA+C2 Device Architecture*.

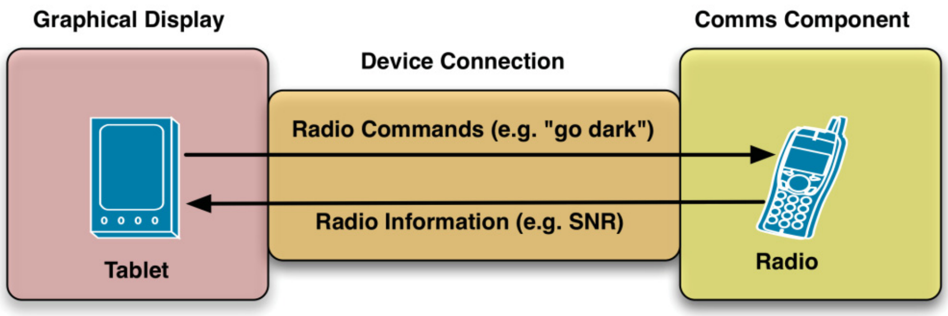

Figure 1: Baseline SA+C2 Device Architecture

This device architecture has three conceptual layers:

1. *Graphical Display*: This interface device will support SA tactical applications by using information that is received by the communication component and in turn supplying information that is generated by the user of the SA+C2 device. This high-level information may include voice, images, or text and is accessed through applications on the tablet itself.

2. *Communications (Comms) Component*: This component allows the SA+C2 device to communicate with other devices via wireless radio signals. Note that there is a distinction between raw network communication and the joining and participation in a MANET. Radio signalling is a hardware function, but MANET participation can be a hardware or software function. As a result, some of the proposed architectures in this study specify MANET participation at the radio (comms component) layer whereas other architectures define MANET participation as a function of the software resident on the graphical display device.

3. *Device Connection layer*: An interface element that allows application-level information and low-level device-specific information to be exchanged between the application/display and radio/signalling components. Examples of the low-level, bi-directional information flows that will take place between the graphical display and the comms component are shown in Figure 1: *Baseline SA+C2 Device Architecture*. These information flows include sending commands to the radio to alter its behaviour, for example:

    a. Go dark: cease all communications;

    b. Go passive: enter a passive scanning mode; and

c. Alter protocol behaviour

The device connection layer must also allow on-board applications to draw from a broad set of radio operational parameters. While this is an existing capability in current handheld / communications unit interaction (e.g., mobiles phones can retrieve and display signal strength), there is a requirement for mobile SA+C2 devices to be able to leverage more sophisticated information from the radio or wireless chipset. For example, mobile SA+C2 applications may require signal-to-noise ratio (SNR) information to support optimal node deployment and network robustness.

Given that the richness of the information that can be leveraged by SA+C2 applications is a function of the information that can be drawn from the communications component, the nature of the information that can be retrieved and commands that can be sent via the device connection layer forms an important element of this study. This study will examine not only what information is currently accessible through this interface but also how the interface can be modified to include a broader set of custom defined capabilities, for example:

1. Currently available radio/chipset operational parameters and metrics in existing COTS/MOTS products;

2. Ability to modify radio protocols and operational characteristics; and

3. Support for the development of custom software or firmware to meet future requirements for tactical networks.

Additionally, while conducting this study specific constraints were identified that have a direct bearing on the selection of an optimal architecture and technology configuration for the envisioned mobile SA+C2 device. These constrains are identified below.

1. For soldiers in the field, there is a preference for solutions that do not impede mobility. In architectures where the graphical device and communications unit are separate elements, wireless pairing/tethering may be preferred over wired connections (although this presents a host of additional issues).

2. In terms of procuring solutions that must be provisioned and supported for soldiers in the field, vendor-based solutions are preferred over open source or custom built technologies. In order to transition solutions to the field there must be a strategy for acquiring and provisioning these devices and this is a capability that is better met by the vendor community.

1.2 Document Structure

The remainder of this report is divided into four sections.

Section 2 provides a high level description of the architectural approaches and associated variants that could form the basis for the SA+C2 device. Each proposed architecture is described in terms of the functions performed by the elements in the solution and appropriate representative hardware is identified for the solution components.

Section 3 provides a detailed description of relevant COTS/MOTS and open source hardware and software packages that could be used to provision the SA+C2 device. Representative technologies from vendors in the radio, tablet and MANET solution space are examined in greater detail and the operational characteristics of the equipment, performance metrics and relative cost are presented for a selection of relevant products.

Note: Section 3 can be omitted for readers that are primarily interested in the analysis and conclusions from this study.

Section 4 provides an interpretation of the information presented in the previous sections and presents, with rationalization, the most viable SA+C2 solution architecture. This section describes the SA+C2 device in its operational context and provides a perspective on extending the capability of the device to meet additional requirements beyond the scope of the initial project.

Section 5 summarizes the study results and provides suggestions for future areas of research.

2 Architectural Specifications

In order to properly describe the individual components for the mobile SA+C2 device in context, it is useful to present a higher level view of the proposed solution. The vision for the device includes a graphical display connected to other devices through a MANET architecture where network connectivity is achieved via radio devices that are linked to the display. From this general description, there are many potential device architectures that can adhere to the solution specification.

This section examines a range of possible component configuration models that can achieve the potential requirements for an envisioned mobile SA+C2 system. Each architectural approach is described in terms of the role of each component, connections that link the individual device components, and the manner by which the MANET connection between devices is achieved.

Each of the solution architectures is described in terms of the unique technical challenges that are presented by the component selection for that architecture. Common challenges that are shared across architectures are similarly identified. A side-by-side comparison of the proposed architectures is summarized at the end of this section. The architectural definitions and associated technical challenges serve as a basis for the component-level analysis in section 3:*Analysis of Current Technologies* and subsequent interpretation in section 4:*Interpretation of Results*.

2.1 Architectural Approaches

Each architectural approach is described in this section with its related variants. Variant architectures all share a common approach in terms of the placement and function of the individual components, but have slight differences in terms of the selection of the individual components. Within each architectural description, all variant architectures share a common set of technical challenges but individual variants may introduce additional complexities.

2.1.1 Tablet Only

The first architecture is also the simplest, as shown in Figure 2: *Architecture 1: Tablet Only Architecture*. It is a "tablet only" device[1] where the integrated radio is used for communication in the MANET and the device's participation in the MANET is controlled through the tablet resident software. Solutions based on this approach leverage the tablet's internal Wi-Fi wireless radio, which is more limited in range and power as compared to an external radio. A full description of the capabilities of tablet-based radios is provided in section 3.2:*Tablet Component*.

In examining a tablet-based architecture, specific areas of interest associated with the challenges of constructing flexible and configurable mobile SA+C2 devices can be identified. These areas of interest are as follows:

[1] For simplicity, the term tablet is used to describe the handheld GUI based component. Non-tablet devices (e.g., smart phones) are also relevant to this architecture but share the same advantages and challenges.

1. User-space processes (graphics-based applications) must be able to access low-level chipset capabilities present in the internal tablet radio. Access to these capabilities may be limited or restricted.

2. Existing device drivers, kernel modules, or firmware may need to be extended to include capabilities needed by SA+C2 devices but not present through the existing interface specification.

3. The existing tablet operating system must provide MANET support or be able to be upgraded or extended to include the needed MANET capabilities.

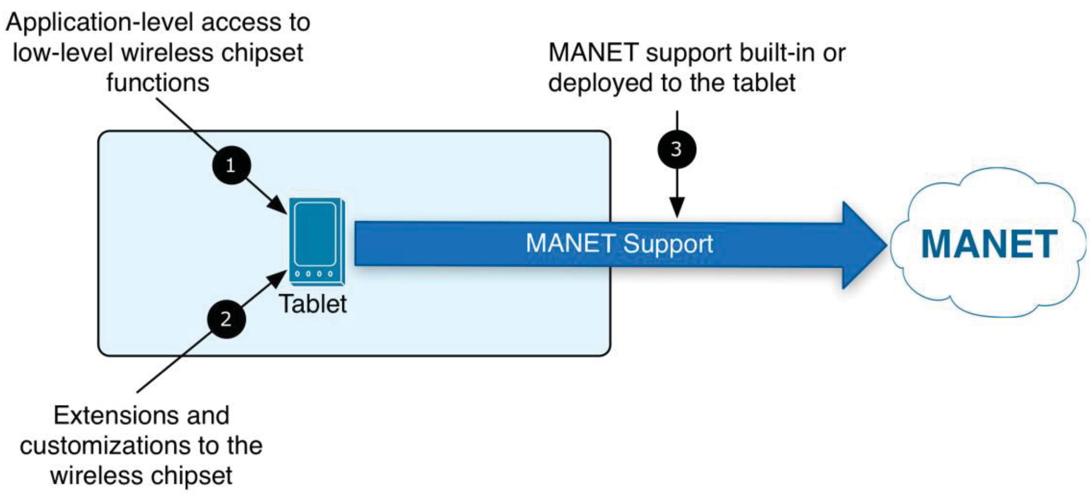

Figure 2: Architecture 1: Tablet Only Architecture

With respect to the last area of interest, concurrent experimental work at DRDC to create a tablet-based MANET has provided evidence that MANET support can be deployed to Android-based tablets. MANET support is not natively part of all Android software releases and currently is only supported in certain hardware/software configurations, as defined in section 3.1.2.2:*Tablet Integrated Solutions*. Third party applications, most notably MANET Manager[2], can supplement the existing Android device deployment to include MANET capabilities. The system and hardware requirements for MANET Manager include:

1. Root access to the device;

2. An OS kernel that supports wireless extensions; and, most significantly;

3. A wireless device driver that supports ad-hoc mode.

Requiring a chip with driver support of ad-hoc mode restricts the list of applicable tablet-based devices that can support the future SA+C2 device architecture "out of the box".

[2] MANET Manager is a Google Play Android app that allows users the ability to enable and configure a MANET for devices in order to connect with similarly equipped devices within range.

2.1.2 Externally Assisted Tablet-based Communications

This approach is characterized by the tablet continuing to be the broadcasting component for MANET communications, but the limited broadcasting range of the internal wireless chip and antenna is mitigated by an adjunct solution element. This approach has two variants.

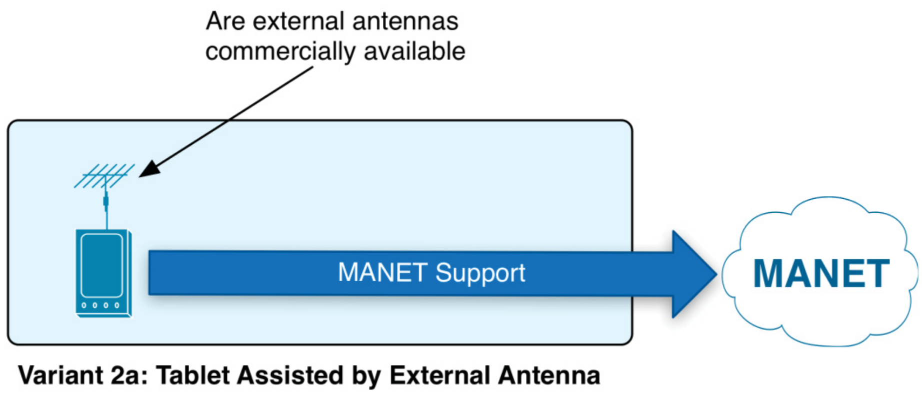

Figure 3: Architecture 2a: Tablet with External Antenna

In one architectural option, shown in Figure 3: *Architecture 2a: Tablet with External Antenna*, the internal radio's broadcast signal is enhanced with an external antenna to extend the broadcast range (transmit and receive) of the internal Wi-Fi radio.

External antennas for cellular devices, known as patch leads, do exist but are rarely provided as a commercial option. As shown in Figure 4: *External Antenna Hardware Modifications* the Samsung Galaxy Nexus has an radio frequency (RF) connector that is accessible by taking off the back cover. A patch lead can be attached to the device to increase the speed and reliability of mobile broadband internet[3].

External antennas for Wi-Fi tablets are uncommon and are primarily driven from the hardware modification community. Frequently, the need for extended Wi-Fi range stems from remote control (RC) drone enthusiasts. In December 2012, a team achieved a new record for Wi-Fi range using a Google Nexus 7 tablet to control a Parrot AR.Drone[4] at a distance of 2.25 kilometers. The necessary modifications to the tablet were extensive requiring the device to be physically opened to gain access to the radio hardware elements, as shown in Figure 4: *External Antenna Hardware Modifications*.

---

[3] As previously stated, external antenna support is not a common feature for tablets. In the case of the Galaxy Nexus, the RF port was intended for device testing purposes only and discovered by the tablet hardware/software enthusiast community with information from the Nexus engineering team.

[4] http://forum.parrot.com/ardrone/en/viewtopic.php?id=6791

Figure 4: External Antenna Hardware Modifications

The original antenna was, in actual fact, removed in favour of a Hawking 13dBi QuadPatch directional antenna resulting in a tablet with impressive wireless range at a cost of mobility as shown in Figure 5: *A Tablet with a Long Range Directional Antenna*.

Figure 5: A Tablet with a Long Range Directional Antenna

In summary, in the absence of general commercial support for external antennas for tablets, there are feasible methods for making modifications to the tablet to provide external antenna support. Some experimentation would be required to determine the practicality of physically altering these devices. The reliability and robustness of the device after modification would most likely be negatively impacted.

In the second variant, a wireless router is added to the solution such that the tablet connects to the router and the signal is repeated, with greater broadcast strength, through to a second network. Each tablet would then be on a separate private network connected to a central network via the routers, which would connect all the individual networks. This architecture is shown in Figure 6: *Architecture 2b: Tablet with External Router*.

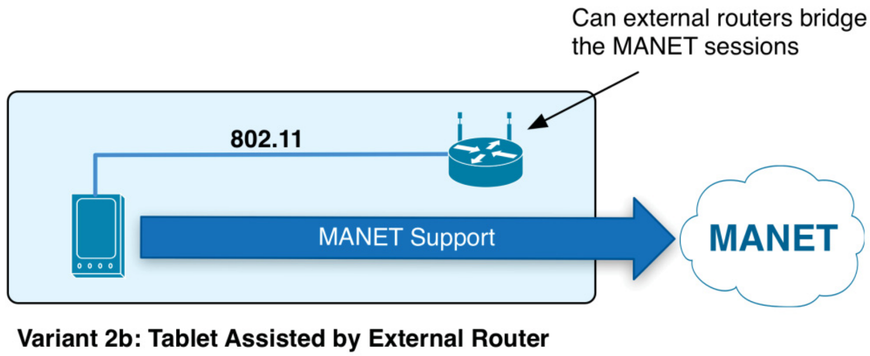

Figure 6: Architecture 2b: Tablet with External Router

Existing products such as the ZuniConnect Travel Router or the ASUS 6-in-1 Wireless-N150 Mobile Router can operate in WISP mode (Wireless Internet Service Provider) that will allow a wireless network to be bridged to another wireless network. Both products are portable with extended battery life rendering them suitable for a mobile deployment.

In both variants, the previously described challenges with tablet-based MANETs and integrated radios components remain. Specifically, there are challenges associated with:

1. Providing applications with access to the low level wireless device interfaces;

2. Updating hardware drives/firmware to include features that are missing from the default interface; and

3. Deploying and configuring the tablet to manage MANET participation.

This last item is made more significant in a router-based architecture. While a router configuration will allow traffic to pass between networks, the MANET routing protocols may be significantly impacted. The proposed architecture, based on a WISP mode router where the tablet connects to the "private" side of the router and packets are sent to other devices over the "public" router interface, means that each tablet is on its own private network segment. As packets leave the tablet to be transmitted to other devices, the router will perform a translation of the network address to map it from the private segment to the public segment, in accordance with the network address translation (NAT) protocol. MANET routing protocols that depend on physical device characteristics that are only visible inside the private segment will not be able to function though a NAT-based router without complex routing tables. Address management and conflict

resolution must also be addressed in a scenario where there are multiple private networks that connect through a common network zone.

2.1.3 Networked Tablet and with External Radio

The variant approaches in this section are characterized by the fact that the integrated radio is no longer the primary transmitting component for the SA+C2 device. An external radio is used to provide communications for the MANET with the expectation that this radio will have:

- Improved operating parameters (e.g., broadcast range);
- A more open architecture supporting the need to access and modify radio configuration parameters; and
- The ability to switch to an alternate radio component if necessary.

In this scenario, participation in the MANET is still a function performed by the tablet device's operating system and network subsystem. This configuration is shown in Figure 7: *Architecture 3a: Tablet with External Wi-Fi Radio*.

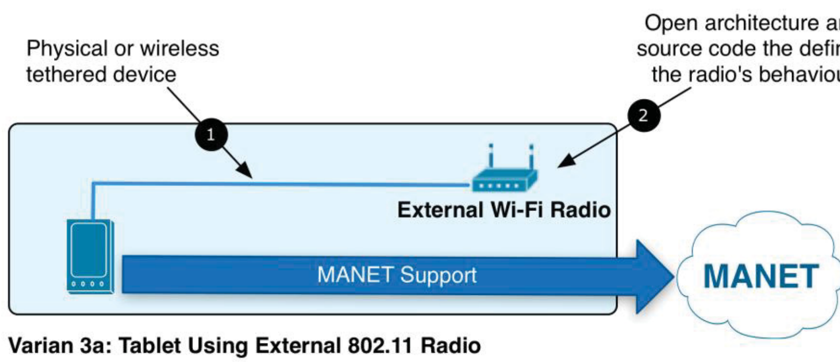

Figure 7: Architecture 3a: Tablet with External Wi-Fi Radio

The first variant of this architecture uses a commercial Wi-Fi radio connected to the tablet to replace the internal wireless radio. These radios are, therefore, limited to the 802.11 media access control (MAC) and physical layer (PHY) specifications. In examining this architecture, two areas of interest are identified.

1. There must be a means by which the tablet and radio are linked. Wireless Wi-Fi products in this space can support a variety of connection mechanisms including:
    a. Physical tethering such as the TP-Link USB-based external radio; and
    b. Wireless linkages such as the Motorola MTP3200 which provides a secure Bluetooth option to connect the radio to handheld devices.
2. To be of value to the SA+C2 solution architecture, there must be a means by which the interface specification and behaviour of the radio can be altered. Sophisticated apps may

need the ability to change the behaviour of the radio and, therefore, the architecture and driver code for the radio must be open and available.

A survey made of leading vendors in the field of land based and mobile radio devices indicates that most radio architectures are either closed by design or indirectly closed through limiting the publication of architectural details. The rationale for keeping radio interfaces closed included:

a. A concern over the violation of the radio's certification status;

b. A concern over exposing a large attack surface through which the radio could be compromised; and

c. Intellectual property concerns.

Nevertheless, there are radio devices favoured by the research and open source development communities that do expose driver source code and architectural designs. Section 3.1.3:*Open Source Radios* provides a description of known radio products whose operations can be accessed and altered through the modification of open source code and published documentation.

The second of a networked tablet with external radio architecture is shown in Figure 8: *Architecture 3b: Tablet with External Full Spectrum Radio*. In this configuration the radio is a full spectrum transmitting device capable of signalling beyond the specification of the set of 802.11 protocols. Radios in this class share the same concerns common to this architecture: how to tether the radio with the tablet and how to access or modify the operation of the radio itself.

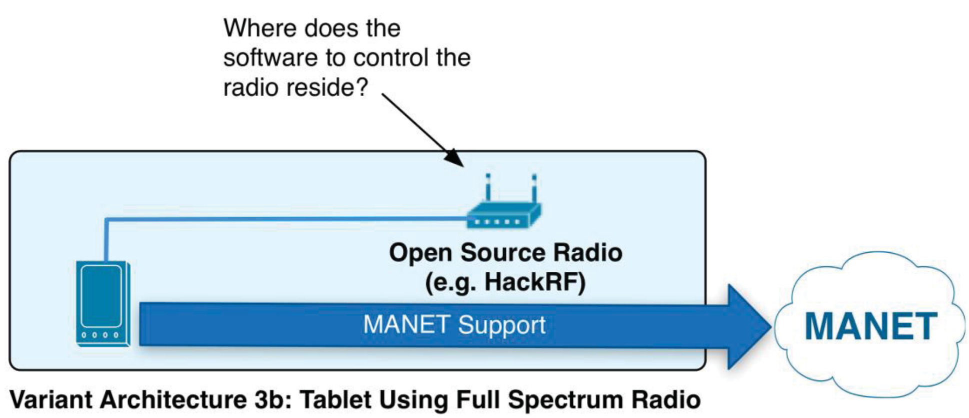

Figure 8: Architecture 3b: Tablet with External Full Spectrum Radio

One prime candidate for this architectural variant is a set of openly published software defined radios (SDRs) such as the bladeRF and HackRF products which are discussed in detail in section 3.1.3:Open Source Radios. Being completely software driven, these solutions can be easily modified [3] and can benefit from pre-packaged software modules for supported protocols.

2.1.4 Tablet with Networked Radio

The final architectural approach leverages the capability of military/commercial radios to not only provide the wireless connectivity but also to manage participation in the MANET. As previously mentioned, commercial and military devices are more closed than community based solutions and for this architecture the degree of control must extend not only to the radio's operating parameters but also to the logic that enables participation in the MANET. Figure 9: *Architecture 4: Tablet with MANET-enabled Radio* illustrates this architecture with the radio being the component that controls MANET functions for the graphical device.

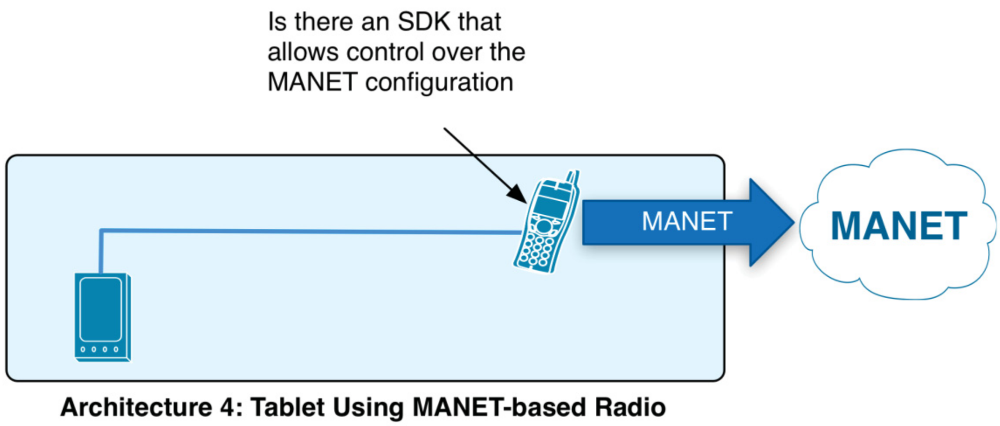

Figure 9: Architecture 4: Tablet with MANET-enabled Radio

COTS and MOTS solutions from technology vendors such as Persistent Systems and TrellisWare meet the technical specifications for this architecture in that they both provide a radio with integrated MANET capability and the ability to connect to graphical display devices.

Section 2.2: Summary of Representative Technologies and Table 2: Summary of Architectural Approaches reviews these six architectural variants and the properties that characterize each approach.

In section 3:*Analysis of Current Technologies*, representative solutions and product offerings are examined for technical capabilities that will allow them to be placed into one of the proposed architectures. Vendor or community-based solutions are summarized to identify the factors that will have a bearing on the selection of the most appropriate architecture and hardware/device configuration solution for the SA+C2 device.

2.2 Summary of Representative Technologies

Figure 10: Review of Architecture Types represents the 4 architectures and their associated variants in context. Note that these architectures can be classified, as shown in Table 1: Classification of SA+C2 Device Architectures, in terms of where the transmitting device is located in the architecture, the nature of the transmitting device and which elements are responsible for participating in the MANET.

Transmitting Device	Tablet manages MANET	Radio Manages MANET
Tablet	• Architecture 1: Tablet Only • Architecture 2a: Tablet With External Antenna • Architecture 2b: Tablet with External Router	
Radio	• Architecture 3a: External Wi-Fi radio • Architecture 3b: External Full Spectrum Radio	• Architecture 4: MANET capable commercial radio

Table 1: Classification of SA+C2 Device Architectures

Table 2: Summary of Architectural Approaches presents the operational characteristics of each proposed architecture. Based on these characteristics, the relative advantages and disadvantages of each option will be discussed in subsequent sections.

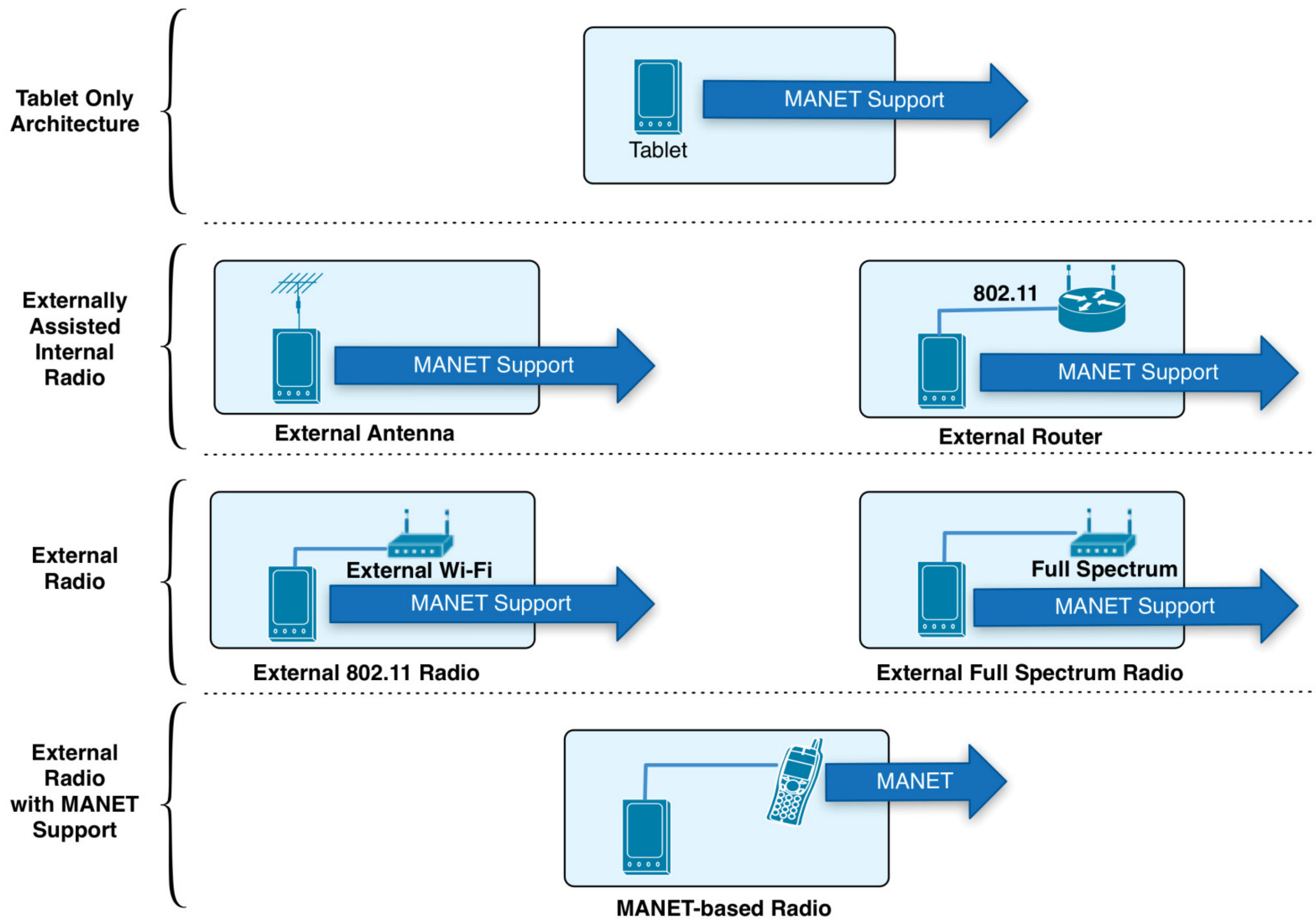
Tablet Only Architecture
Tablet
MANET Support
Externally Assisted Internal Radio
MANET Support
External Antenna
802.11
MANET Support
External Router
External Radio
External Wi-Fi
MANET Support
External 802.11 Radio
Full Spectrum
MANET Support
External Full Spectrum Radio
External Radio with MANET Support
MANET
MANET-based Radio

Figure 10: Review of Architecture Types

Table 2: Summary of Architectural Approaches

Architecture	Arch#	Performance	Configurability / Modification	Ease of Use	Support	Examples
Tablet Only	1	Short Broadcast Range Wi-Fi only	Source code for MANET and some drivers exists	Simple architecture	Community supported software	Google Nexus 7
Antenna Assisted	2a	Extended broadcast range		Attached antenna may interfere with ease of use	Manual hack required	
Router Assisted	2b			Complex physical and network configuration	Available but non-standard MANET configuration	
External Wi-Fi Radio	3a		Source and architecture for radio exists for some devices	Attached devices typically physically tethered	Community support	TP-Link USB Wireless
External Full Spectrum	3b	Extended range Full Spectrum				HackRF, bladeRF
External Radio with MANET Support	4	Long Range Radio Full Spectrum	Limited	Wireless radio and tablet connectivity options available	Available and vendor support for product capabilities	TrellisWare, Persistent Systems

3 Analysis of Current Technologies

This section provides a detailed description of relevant COTS/MOTS and open source hardware and software packages that could be used to provision the SA+C2 device. Representative technologies from vendors in the radio, tablet and MANET solution space are examined in greater detail and the operational characteristics of the equipment, performance metrics and relative cost are presented for each product.

Note: *This section can be omitted for readers that are primarily interested in the analysis and conclusions from this study.*

The SA+C2 device architectures defined in the previous section raise specific questions related to how the solution is provisioned, connected at a hardware level, integrated at a device/networking level and used to create applications. These questions are addressed in this section.

3.1 Radio Component

This section examines potential options for the radio component of the mobile SA+C2 device as it relates to the proposed architectures. Figure 11: *Available Radio Components* shows the potential sources for the radio component and identifies the sections where these components are discussed within the report.

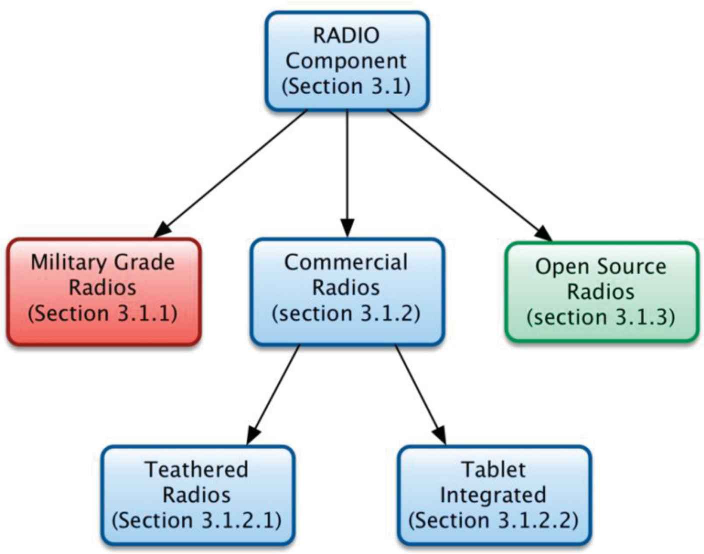

Figure 11: Available Radio Components

In the course of investigating representative radio offerings from each source (MOTS, COTS and open source) the following areas of interest were used to determine the applicability of each solution.

1. The degree to which low-level control be exerted over the onboard radio chipset.

2. The need for kernel or device driver modifications to extend control over the local radio, the manner by which these modifications are pushed/integrated to the device and the impact these modifications have on the tablet.

3. The typical device specifications for tablet integrated radios, including: range, throughput, frequency range, power, size and protocol support.

4. The accessibility of driver level functions of external radios and the capabilities that are extended though driver interfaces.

5. The feasibility of leveraging device driver interfaces in the design and implementation of SA+C2 applications to send commands to the low-level radio interfaces.

6. The mechanisms by which the tablet can physically interface (tether and/or pair) with the external radio and the protections that can be put in place to secure this connection.

7. The existence of any device driver kits (DDK) that would allow the deployment of customized drivers in support of SA+C2 requirements and the ease by which this DDK can be used to implement modifications.

8. The ability for tablets to leverage open source directions directly without the need for a secondary processing device to manipulate signalling and protocol behaviour.

9. General device specifications of external COTS/MOTS radios.

3.1.1 Military Grade Radios

Many military suppliers have products that provide built-in MANET support. Some vendors have complete solutions whereas other vendors have components that could provide the basis for developing a solution given a sufficiently detailed requirements specification.

Though the radios described in this section are considered military products, many have civilian applications. Several of the manufacturers have P25 radios, which is an emerging standard for public safety and emergency response communication. The advantage of P25 is that it is possible to mix equipment from different manufacturers, while maintaining communication exchange of critical information such as location.

Most of the radios listed in this section support a form of tethering for connecting to an external device such as a tablet. Usually this connection is via a USB cable, but Bluetooth is also supported in some configurations.

Throughout this section, links are provided for access to product specifications or technical articles that are relevant to the technology. Several of the products were launched or upgraded during the course of this investigation and represent the state of technology as of this writing.

3.1.1.1 TrellisWare Technologies

TrellisWare is focused on advancing communications technology by providing products that leverage improvements in digital communication theory and electronics density. TrellisWare specializes in advanced communication algorithms, waveforms and turnkey communication

systems. Their products are geared towards military and commercial applications in harsh environments and are ruggedized for tactical deployments.

On September 27, 2013 TrellisWare received a U.S. Navy contract worth up to $11.7 Million over 5 years to provide support in developing mobile ad-hoc networking solutions. There was no competition for the contract since only TrellisWare could satisfy the Navy's requirements. A selection of their relevant products and technologies is presented below.

<u>CheetahNet TW-220</u>

Table 3: TrellisWare CheetahNet TW-220 Specifications

<table>
<tr><td>Product Type</td><td colspan="2">Wideband networking radio</td></tr>
<tr><td>Product Features</td><td colspan="2">MANET support and interfaces for Ethernet, USB, and Bluetooth.</td></tr>
<tr><td rowspan="7">Specifications</td><td>Range</td><td>21 km per hop
8 hops maximum for a full range of 167 km</td></tr>
<tr><td>Throughput</td><td>2 Mbps</td></tr>
<tr><td>Frequency</td><td>905-925MHz
1775-1815MHz</td></tr>
<tr><td>Power</td><td>Less than 2 Watt Peak</td></tr>
<tr><td>Security</td><td>AES256 encryption</td></tr>
<tr><td>Form Factor / Weight</td><td>12.7 x 6.6 x 3.8 cm
0.5 kg</td></tr>
<tr><td>Notes</td><td>Available applications include: PTT voice, streaming IP video, IP data, PLI
Interfaces include: Ethernet (RJ-45), USB mini A/B, Bluetooth, 14 hour battery</td></tr>
<tr><td>Product Publications</td><td colspan="2">http://www.trellisware.com/wp-content/uploads/TW-220-CheetahNet-Product-Bulletin.pdf</td></tr>
<tr><td>Applicable Architecture</td><td colspan="2">Architecture 4: External Radio with MANET Support</td></tr>
</table>

CheetahNet is a wideband networking radio unit that provides voice, high-speed networked data, and full-motion video simultaneously. It is completely self-configuring, with no setup or management needed. Networks are self-forming and self-healing with less than 1 second required to join the MANET. The MANETs that are established route information between nodes using a transparent routing protocol that is abstracted from the user.

The CheetahNet device can connect, through separate dongle interfaces, to data devices including tablets. In the case of the USB dongle, the radio can provide power to the connected device and can serve as a USB host to store network data on a flash drive. The prime role for the

CheetahNet product is rapid deployment of wideband networks in harsh conditions. This makes the radio appropriate for both commercial emergency response and military scenarios.

CUB TW-400

Table 4: TrellisWare CUB TW-400 Specifications

Product Type	Wideband networking radio	
Product Features	MANET support and interfaces for Ethernet, USB, and Bluetooth.	
Specifications	Range	21 km per hop 8 hops for a full range of 167 km
	Throughput	20 Mbps for voice/data and location (dual band)
	Frequency	1775-1815 MHz 2200-2250 MHz
	Power	2 Watt Peak
	Security	AES256 encryption
	Form Factor / Weight	10 x 6.4 x 2.3 cm 280 g
	Notes	Many accessories and sensors available Applications for ground sensor networks, remote sensor access small tactical robot and PLI Tracking
Product Publications	http://www.trellisware.com/wp-content/uploads/TW-400-CUB-Product-Bulletin.pdf	
Applicable Architecture	Architecture 4: External Radio with MANET Support	

This product is a smaller version of the CheetahNet with a much higher data rate, remote controllable, and support for an open API for solution developers. It includes multi-channel push to talk, IP data, position tracking, and live video streaming. The device also supports the addition of sensor units for extending the capability of the radio, including: BNC video and trigger sensors. Whereas the TW-220 is an entry level radio, the higher priced TW-400 provides more capabilities.

WildCat II TW-130

Table 5: TrellisWare WildCat II TW-130

Product Type	Amplifier & dual channel radio	
Product Features	Dual radio quad-band tactical MANET device for connecting two networks (two complete quad-band wideband radios).	
Specifications	Range	21 km per hop

		8 hops for a full range of 167 km
	Throughput	40 Mbps for voice/data and location (dual band)
	Frequency	30–512 MHz, 1755–1815 MHz, 2200–2250 MHz
	Power	8 W Peak (x2 channels)
	Security	AES-256 COMSEC
	Form Factor	14 x 12.7 x 5 cm 1.5 kg
	Notes	Vehicle mount form factor
Product Publications	http://www.trellisware.com/wp-content/uploads/TW-130-WildCat-II-Product-Bulletin.pdf	
Applicable Architecture	None, may act as a bridge between dismounted groups	

The WildCat II is the smallest dual channel tactical MANET on the market. It is less than 1.3 kilograms with 2 complete radios permitting the interconnection of 2 networks. It can be remotely controlled across the networks. It supports the same wideband MANET as the CheetahNet and CUB handhelds. Both radios support narrowband voice and wideband networked modes with aggregate data rates up to 20 Mbps. VHF/UHF/1800/2200 MHz bands range in power outputs from 0.1 Watts up to 2 Watts peak in low power operation, and up to 8 Watts in the 1800/2200 bands using internal power amplifiers.

Additional Notes

The TrellisWare devices have built in support for MANET and have an open API for developers. There are accessories including antennas and dongles for various interfaces. Software tools include radio configuration and network topology information via a standard browser interface. The company claims scalability to 1000's of units by removing routing tables, evaluated with over 200 users, using Barrage Relay Networks, a topic discussed in more detail in section 3.3.2:*Radio-based MANET Configuration*.

An attempt was made to contact TrellisWare to gain additional information related to the development API for their radio products. The Vice-President of Wireless Systems indicated the following:

> *Yes, we do have an API for our CUB units that output a wide range of network visualization data (GPS locations, network links, link quality, range between units, unit battery life, audio channel, etc). This data is available to all of our active customers through our support site. We don't currently have a mechanism to offer access to any of that data to non-customer 3rd party developers at this time, though.*

Short of purchasing their product, no further information regarding the developer Application Programming Interface (API) could be obtained from TrellisWare without a non-disclosure agreement.

3.1.1.2 Persistent Systems

Persistent Systems (PS) is a US company based in New York City. They offer a proprietary mobile ad-hoc networking solution (Wave Relay) that is an adaptive mesh network architecture for use in difficult environmental conditions. PS has both Department of Defence and commercial customers. They are rated dual use under the auspice of the Department of Commerce.

MANET support is built into their products and includes management capabilities via web interfaces, and network visualization using Google Earth. A management API uses the Hyper Text Transfer Protocol (HTTP) and EXtensible Markup Language (XML) as well as monitoring that is supported via the Simple Network Management Protocol (SNMP).

All Persistent Systems products have been engineered to meet the company's design priorities, including:

- Scalability to a large number of devices;
- Cost-effectiveness as a single source solution designed by Persistent Systems;
- High performance due to peer-to-peer topology for shortest data path;
- Rapid deployment as the Wave Relay mesh architecture operates on OSI Layer 2 (data link);
- Fault Tolerance as all nodes are meshed and there is no dependency on a single node.

A selection of their relevant products and technologies is presented below. The PS products are intended to be a complete solution and meet all customers' requirements out of the box. Per client customization is possible, but would require a more in-depth conversation with the PS account managers.

Android Kit

Table 6: Persistent Systems Android Kit

Product Type	Connecting Kit that allows Android devices to access PS radios
Product Features	A USB/Ethernet connection to an Android device with a custom App.
Product Publications	http://www.persistentsystems.com/pdf/GovernmentAndMilitary_AndroidKit_SpecSheet.pdf
Applicable Architecture	Provides the connectivity between the radio and tablet in Architecture 4

PS has created a hardware/software bridge through which stock Android phones and tablets can be used to display information from the PS radio suite. The handset device connects to the radio through a USB to Ethernet cable which plugs into a port on the PS radio. The handheld device is updated to use a custom, ruggedized Android kernel and an application (WAveSA) to allow the presentation of radio source information and control over radio operation, including: displaying video feeds, determining location/position data, and configuring network status via the Android device. The WAveSA App Features and configuration options include the following:

- Position location of each node;
- Link status between all nodes;
- View phone-to-phone video or video from the MANET;
- Multicast Group Chat;
- Real-time notification of incoming chat requests & available video feed;
- Breadcrumbing of selected nodes;
- View GPS status;
- Change of audio channel;
- Replay of last audio message;
- Control audio volume;
- See connection status;
- Set IP address, subnet, and default gateway;
- Configure Username/call sign and Cursor on Target (CoT) settings;
- Enable USB Host Charging; and
- Network Configuration through Web Management Interface Shortcut

The tablet GUI product was just added to the PS catalogue. It is packaged as a kit with the tablet, an Android App, cables, and case. The software is compatible with Samsung Note 1 & 2. The connection is via USB and it is encrypted in the same manner as the radio links. The App handles maps and video and uses PS's own proprietary API. Bluetooth support between the tablet and the radio is not currently available but is being considered by the PS technical team.

In the PS product suite, every node has an IP address and every node, be it radio, board or router, runs the same Wave Relay software.

Man Portable Unit GEN4

Table 7: Persistent Systems MPU GEN4 Specifications

Product Type	Personal Role Radio
Product Features	A wearable form factor radio for the dismounted user, which directly supports mobile ad-hoc networking for transfer of data, video, and voice.

Specifications	Range	3.25+ km with omnidirectional antenna
	Throughput	37 Mbps UDP, 27 Mbps TCP (20 Mhz)
	Frequency	763-778 MHz 907-922 MHz 2312-2507 MHz 2412-2462 MHz 5180-5320,5500-5700, 5745-5825 MHz
	Power	4.2 W (average consumption) / 600mW output
	Security	FIPS 140-2 Level 2, AES-CTR-256 with SHA-512 HMAC
	Form Factor	11.7 x 7.6 x 3.8 cm 0.5 kg
	Additional	Support for external sensors, cameras
	Pricing	\$6500 - \$7000 depending on the kit (antenna selection)
Product Publications	http://www.persistentsystems.com/pdf/MPU4_GovernmentAndMilitary_SpecSheet.pdf Product pricing catalogue is available but not redistributable	
Applicable Architecture	Architecture 4: External Radio with MANET Support	

Quad Radio Router

Table 8: Persistent Systems Quad Radio Router

Product Type	Multi-Network MANET Router	
Product Features	A multi-channel, multi-hop backhaul for connecting nodes in a single solution for mesh networking. Includes four embedded radio modules that operate in the 2.3 – 2.5 GHz and 5 GHz frequency bands and supports 16 channels of push-to-talk. The router product is targeted at both tactical (rapid deployment) and vehicular networks.	
Specifications	Range	When combined with the Wave Relay Tracking Antenna System, the Quad Radio Router will track

		airborne nodes over 160 km away.
	Throughput	27 Mbps of TCP throughput across multiple wireless hops.
	Frequency	2.3 – 2.5 GHz and 5 GHz standard 700 MHz, 900 MHz, 3.5 GHz, and 4.9 GHz optional
	Power	<16W consumption, 2W transmit
	Security	Integrated Hardware Encryption
	Form Factor	21.6 x 15.2 x 5 cm 1.4 kg
	Additional	• FIPS 140-2 Level 2 Validated by NIST • Network wide firmware upgrade • G.711 codec for radio-over-ip
Product Publications	http://www.persistentsystems.com/pdf/ps_quadradio.pdf	
Applicable Architecture	Provides the connectivity between the radio and tablet in Architecture 4	

The Quad Radio Router has four separate wireless radios for network routing, plus 5 10/100 Mbps Ethernet ports, a connector for push-to-talk headsets, and 2 serial ports for serial-over-Ethernet. Multiple interface options are provided, including, antennas, audio, GPS, and Power over Ethernet (PoE).

Management Tools

In additional to their hardware solutions, Persistent Systems has several management tools for their MANET products:

- Web Based Management – a tool for network configuration and management integrated into all Wave Relay routers;

- Google Earth Based Network Visualization – complete integration with the Google Earth Server permitting real time monitoring of the network. Locations of nodes and quality of links are served directly from the router: both to management console and to individual handheld units that are running the PS Android Kit WaveSA app.

- Management API – allows programmatic management by third parties so customers can integrate control into their own products. The API uses HTTPS and XML or HTML;

- SNMP Management – mean standard SNMP management tools may be used to monitor the system, including temperature, and voltage.

Additional Notes

An attempt was made to contact Persistent Systems to gain better insight into their products, the degree to which those product architectures were open and the possibility of altering the devices for the development of new capabilities. A PS business development specialist was able to provide additional product sheets, which have subsequently been made available on their web site, and a product catalogue.

PS handles product updates in a formalized process. They upgrade the firmware every 2 months; this firmware encodes all of the IP networking (i.e. Wave Relay) into the device. The MANET technology is based on their own proprietary Wave Relay algorithms. PS claims that they have excelled in evaluations against other competing products, although the details about how their networking algorithms are optimized are subject to IP restrictions. API support is provided for customers who request it. As with TrellisWare, further information regarding the developer API could not be obtained from PS without a non-disclosure agreement.

3.1.1.3 Harris Tactical Communications

Harris Tactical has a selection of radios and associated equipment, including satellite networking. They have NSA certification for Top Secret and below for some equipment and frequencies. There are two devices that appear interesting for software control and MANET applications.

RF-7800S-TR Secure Personal Team Radio

Table 9: Harris RF-7800S-TR Specifications

Product Type	Personal Role Radio	
Product Features	Team-oriented secure digitized voice and data. Digital wireless network allows reliable communications and robust, long-range operation even in harsh environments. Full duplex in the 350-450 MHz band with priority-based voice conferencing.	
Specifications	Range	2-3 kilometers per hop in open terrain, half that in urban or harsh terrain
	Throughput	Up to 256kbs
	Frequency	250 – 450 MHz
	Power	2 watts (adjustable)
	Security	AES256 (FIPS-197) Citadel256
	Form Factor	17.1 x 7.8 cm 300 g
	Additional	Upgradable software via USB port 12 hour battery life

		MIL-TSD-801F compliant
Product Publications	http://pdf1.alldatasheet.com/datasheet-pdf/view/312542/HARRIS/RF-7800S-TR.html	
Applicable Architecture	Architecture 3: External Radio	

A USB data interface allows connection of Windows, Linux, or Android devices for data applications. Remote Network Driver Interface Specification (RNDIS) over USB support is provided to extend additional virtual Ethernet to Microsoft-based devices. A wireless port allows remote control of the radio, although no information is provided about what level of control is available via the wireless or USB ports.

<u>AN/PRC-152A Wideband Networking Radio (Falcon III)</u>

Table 10: Harris AN/PRC-152A Specifications

Product Type	Wideband Networking Radio	
Product Features	The AN/PRC-152A radio is a networking handheld providing simultaneous voice and data with backwards compatibility to legacy radios, and USB and Ethernet connectivity with MANET support. With IP networking the radio data applications include, video and data, situational awareness, mapping, text and email, and applications. (No information on the applications is supplied.) The radio utilizes ad-hoc networking for automatic and transparent relay, including automatic network healing. It is certified for TOP SECRET by the NSA. The PRC-152A can automatically form a MANET in UHF bands with a bandwidth of 1.2MHz. A Harris representative claims this radio has worked with up to 30 nodes (with a commensurate sacrifice in network throughput). With 10 nodes in the MANET, they claim you could stream low-quality video among the nodes.	
Specifications	Range	Up to 8 km
	Throughput	Increased data throughput over the PRR product but exact performance numbers not provided.
	Frequency	Narrowband: 30-512MHz Extended Narrowband: 512-520MHz, 762-870MHz (P25 and AM/FM) Wideband: 225-450MHz
	Power	250mW to 5W

	Security	Sierra based Type-1 encryption, certified TOP SECRET and below
	Form Factor	7.4 x 24.4 x 4.8 cm 1.1 kg
	Additional	Harris Adaptive Networking Wideband Waveform
	Pricing	$5,000 USD / unit
Product Publications	http://rf.harris.com/media/AN-PRC-152A_DataSheet_web_tcm26-18518.pdf	
Applicable Architecture	Architecture 4: External Radio with MANET Support	

The PRC-117G is a man-pack version of the 152A with the same general capabilities as the handheld except it is higher power (20W versus 5W) and can support 5MHz or 1.2MHz bandwidth.

The PRC-152A class of device supports simultaneous voice and high-speed networked data using the proprietary Harris Adaptive Networking Wideband Waveform (ANW2) and the Soldier Radio Waveform (SRW). ANW2 uses protocols that do not require the presence of a designated network control station; each radio automatically discovers and joins an authorized network. Ad-hoc networking allows automatic and transparent relay through a central linking station.

In addition to the radios, Harris has a ruggedized tablet that interfaces with both radios. This tablet is capable of displaying the unit's position (using GPS) and comes pre-loaded with several lightweight apps, however the app functionality and ability to display the positions of other allied radios is unknown. Harris also has a lightweight tactical video solution that uses a camera mounted on the soldier's helmet and a Harris video processor to gather and share video over the radio network.

3.1.1.4 Thales Group

Thales Group has several radios of potential interest, some of which include networking data support.

Cougar Team

Table 11: Thales Cougar Team Specifications

Product Type	Secure Personal Radio
Product Features	The Cougar Team is a secure networking radio. It is a compact radio featuring Bluetooth or wired connection for interconnection to 3G and IP networks. It is a SDR (software defined radio) featuring AES encryption and it requires no infrastructure (MANET). Cougar Team unit is very low profile: it weighs 85 grams and is smaller than a deck of playing cards. It operates in the 866 MHz

	band and has a LPI (Low Probability of Intercept) waveform. The Cougar automatically establishes a MANET that can accommodate up to 28 nodes and a maximum of 3 hops.	
Specifications	Range	1.7 km (open terrain)
	Throughput	Not Specified
	Frequency	868MHz
	Power	Not Specified
	Security	Uses COTS crypto (AES-based)
	Form Factor	8.0 x 4.5 x 20 cm 85g
	Additional	Push-to-Talk capability
	Price	$1100/unit
Product Publications	https://www.thalesgroup.com/sites/default/files/asset/document/3565_tha_cougar_team_lr_2.pdf	
Applicable Architecture	Architecture 4: External Radio with MANET Support	

The Cougar Team can pair with a smart-phone to permit the connectivity architecture shown:

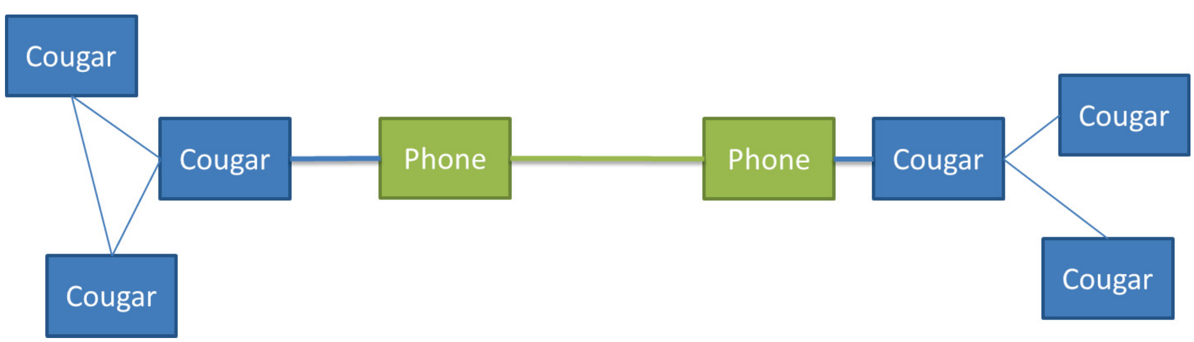

Figure 12:Thales Cougar Team Networking Structure

The St@rMille radio

Table 12: Thales St@r Mille Radio Specifications

Product Type	Personal Role Radio	
Product Features	Handheld solution for intra-squad communications, able to be used in stand-alone configuration or easily integrated in a soldier C4I sub-system for advanced soldier applications. This is not a MANET radio but is "quasi-ad hoc", with the devices capable of performing relay, but with pre-programmed routes. Product operates in the 325 to 470 MHz range, full duplex.	
Specifications	Range	1.5 km (open) / 500 m (harsh)
	Throughput	1000 kbps
	Frequency	325 to 470 MHz
	Power	2 W nominal
	Security	AES256 / MIL-STD-810F
	Form Factor	7.5 x 14.1 x 3.7 cm 370g
	Additional	V24/V28 USB/Ethernet Audio and PTT main
Product Publications	http://www.ste.com.my/pdf/Star%20Mille%20-S_english_V-B.pdf	
Applicable Architecture	Has features in support of Architecture 4 but is not sufficiently tied to MANET standard protocols.	

The radio and GUI are connected via Ethernet through a hub, with each device having a unique IP address as shown:

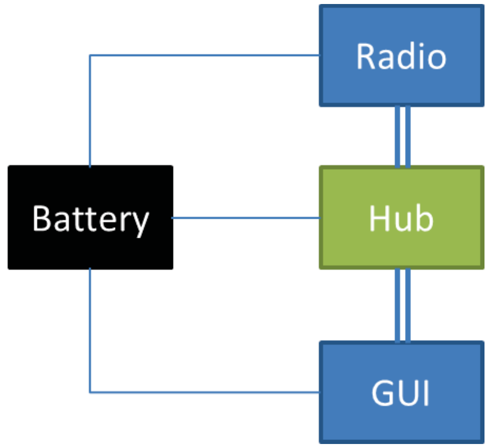

Figure 13:St@rmille Device Networking

Thales has a GUI that runs on both Android and Windows 8 platforms. It is possible to swap out the St@rMille radio with any other radio, as long as it has an Ethernet port. The GUI is not accessing anything special about the radio; in this configuration, the radio is simply serving as a transport.

Additional Notes

Thales offers Battle View: a software product for visualization of location information and situational awareness. It delivers a common operating picture capability to commanders and headquarters. The software runs on Windows platforms, both PC and tablets, and supports an "overlay" concept to display relevant situational awareness data.

3.1.1.5 SELEX ES

The main radio of interest provided by SELEX EX is the Soldier System Radio which is an enhancement to their baseline Personal Role Radio line of products.

Soldier System Radio H4876

Table 13: Selex ES Soldier System Radio

Product Type	Personal Role Radio	
Product Features	The SSR builds on the key design features of the Personal Role Radio (PRR), while enhancing the functionality and performance for in-theater operations. The SSR has twice the range of the SELEX PRR.	
Specifications	Range	1 km urban environment / 2 km open terrain
	Throughput	Not specified
	Frequency	856MHz to 900MHz 350MHz to 450MHz
	Power	Peak output 500mW
	Security	AES256 / Mil-STD-810
	Form Factor	16.0 x 6.8 x 3.5 cm 300g
	Additional	USB 2.0 or V24 Serial port interface
Product Publications	http://www.selexelsag.com/internet/localization/IPC/media/docs/SOLDIER-SYSTEM-RADIO-H4876.pdf	
Applicable Architecture	Architecture 4: External Radio with MANET Support	

A key feature of the SSR is its configurability for cost and compatibility advantages. The SWave handheld (Selex's family of software defined radios) features MANET support, and includes USB and Ethernet interfaces. It provides wideband secure voice and data services. The integrated GPS can be used or the radio can interface with an external GPS. Control is via a graphic display and keyboard or via cable connected remote.

The SWave handheld (HH) features an AES-256 crypto engine and a built-in full IP stack for integration with external networks and IP-based applications. There are tools for radio configuration and SNMP remote management.

The SWave HH can be configured for specific waveforms, the software modules that define the operation of the radio. One such waveform, the SelfNet Soldier Broadband Waveform is a multi-hop MANET (255MHz-512MHz) for squad/platoon operations. It can establish a network of up

to 50 nodes and up to 5 hops and the topology is automatic and dynamic for mobile operations. Voice and data services are simultaneous with configurable QoS policies and priority features.

While the data sheets supplied for the SSR indicate that it has an ad hoc self-healing capability, it seems the radio operates more as a pre-configured relay than as a fully automated MANET or mesh. If this radio is of interest, it would be valuable to confirm how much of its relay capability is truly automated versus pre-configured.

A software application can take both the Radio Configuration Data, generated by the Selex Network Planning Tool, and the Encryption Keys, generated by the Key Generation Tool, and pass it to the SSR Plus radio; however, this represents the limit of the radio's ability to be customized through a programmatic interface.

3.1.1.6 Other Notable Technology Providers

Motorola

Motorola indicated that a set of existing Motorola product offerings could be combined to create a mobile SA+C2 device. Motorola said they have been involved with DRDC on similar R&D projects before and the stance from Motorola was that they have extensive integration experience and could develop the device being investigated by leveraging existing in-house components. They reiterated they were capable of developing a solution from their existing technology given a set of requirements. Product specification details were available but are not presented in a format that would be very useful for third party integration or development.

The list of applicable components includes the following:

1. The AME-1000 is a secure telephony product that combines the benefits of hardware-based cryptography and certificate management with a software-based secure voice application and a commercial off-the-shelf mobile phone.

2. Secure Bluetooth: a means to create an encrypted pairing between devices including the ability to carry voice communications.

3. Ruggedized Touch Computers such as the TC55 and ET1.

4. The AP7181 Mesh Wide Area Network high-performance, multi-radio 802.11n access point to enable a mesh architecture with efficient routing, low latency, low routing overhead, and high-speed handoffs. The Motorola networking solutions are, however, targeted to MAN and WAN deployments rather than infrastructure-less ad-hoc networking.

Motorola offers the LEX700 Mission Critical Handheld that hosts always-on public safety applications that are connected through the LTE network infrastructure. The LEX700 is touted as having the best of both worlds: a ruggedized handheld device tailored for public safety with the ability to leverage the latest public safety applications for the Android operating system. Most significantly for this study, the LEX700 can be linked to the Motorola APX7000 P25 personal radio allowing such applications as push-to-talk to be brought to the handheld.

Motorola does have device management as part of an API but does not usually distribute this outside of their IP partnerships. In discussions, the issue of an NDA was raised and they said under such terms the API could be released, but were quick to add that it is not something that has been written for external use, being more a set of design notes, and they were not convinced that the DRDC research team could make any use of it without a substantial effort.

General Dynamics has two products of potential interest: the Pathmaker radio and a tactical LTE solution.

The Pathmaker Radio is a hand-held MANET offering from GD from their "Fortress" suite of products. GD acquired Fortress Technologies in 2011. The Pathmaker operates on 802.11 (Wi-Fi) frequencies and comes with full mesh self-healing / self-forming capabilities. The datasheet for the Pathmaker radio does not provide any indication of the range of the radio, though the sales associate contacted indicated that the range was larger than one might expect from 802.11.

In addition to the Fortress products, GD is working on an LTE (Long Term Evolution) suite of products for Public Safety applications; these are not mesh radio products, however, and pre-suppose the existence of a support infrastructure.

Raytheon provides DH500 MicroLight: a miniature modular software defined radio with support for MANET, situational awareness, and encryption. The radio supports self-forming / self-healing networking to automatically reconfigure the network as users join, exit, re-join, and move. The radio operates in various bands from 225 – 2000 MHz. The radio supports several encryption options from commercial AES to Type 1 for classified transmission. The DH500 MicroLight radio can be paired with a Sagem computer/display which provides a networking layer and enhanced routing protocols. The system also includes a near-eye eyepiece, which incorporates a camera and a simple finger interface acting as a mouse, providing an alternative to the tablet display.

Ultra Electronics has two products of interest that play in the radio and radio-based situational awareness space: ForceWatch and RadioBridge.

Force Watch is a situational awareness application for Android that integrates into existing networks. Users can mark events or locations on a map, input details about the event using a pop-up window, keep historical data, and track/colour neighbouring nodes. The application also allows users to submit location-defined intelligence reports. ForceWatch is radio agnostic (WI-FI/4G/ tactical radios). It has position tracking capabilities for GPS-enabled devices, and uses a proprietary technology for GPS-denial environments. Additionally, this product is notable for the following characteristics.

1. It provides geo-SA to dismounted units, although the prime use is geared towards first responders rather than military.

2. The solution is software focussed rather than being part of a hardware/software kit.

3. Their solution for sharing SA data among the units relies on a central server. That is, the data is not distributed among the units, but goes to a server first and is distributed out from there. Hence, if disconnected from the server, units will not receive updates from other devices.

4. They have paired with a company (TRX) to provide GPS-denied geo-location services. This relies on pre-placed sensors and externally connected inertial sensors.

5. ForceWatch also feeds the geo-picture back to a HQ, where it is displayed on a management platform.

RadioBridge is a device for integration of radio voice, data and telephony into the IP network. The RadioBridge integrates 4 to 8 radios, a communication switch, and a call manager into a single compact, lightweight and low-power unit suitable for vehicles, ships and airborne systems.

Rockwell Collins has vehicle-level solutions, but does not currently produce a handheld radio for tactical MANETs. According to contacted staff, their product development department is working on a man-pack radio (called the "155") but this is not yet commercially available.

They produce the Subnet Relay solution, a layer 2 relay solution to achieve ad hoc networking (ratified as NATO STANAG 4691). The hardware is quite large; the sales associate indicated this is typically for use in vehicles or naval units—not for man-packs or handheld use. The associate indicated that the Subnet Relay solution would be used in DLCSPM's planned upgrades to the Combat Net Radio (CNR-E).

3.1.2 Commercial Radios

Commercial radios are an alternative to the military radios focused on in the previous section. They are products that are easy and less expensive to procure through local or online electronics suppliers. The division between military and commercial radios is somewhat arbitrary. For example, several of the radio products, such as those from Persistent Systems, are sold with both standard and hardened packaging for commercial and military applications, respectively.

Choosing a commercial product over a military alternative has several advantages:

1. Reduced cost: commercial products are often much less expensive;

2. Increased availability: commercial products are easy to purchase;

3. Large selection: there is a huge variety of commercial offerings;

4. Frequent refresh: the products in this category are frequently updated;

5. Community support: a large user community means getting help is easy; and

6. Aftermarket modification: the community supplies many customizations.

A consequence of these factors means that it is much easier and less expensive to develop technology demonstrations with commercial products versus military products. Furthermore, if techniques are being developed for non-military applications, this is the technology that others will be using and is the technology more likely to be encountered on a day-to-day basis.

Throughout this section, links are provided for current information on these products. Commercial products benefit from frequent updates, although often the products are changed with little public discussion. It is common to see a device released through several iterations and for the device to have the same specifications but to leverage different internal hardware components.

3.1.2.1 Tethered Solutions

Tablets have integrated 802.11 Wi-Fi radios but these typically are both low sensitivity and low power output, and they are not replaceable nor are external antenna connectors provided. To eliminate these shortcomings it is possible to use a tethered radio as an upgrade to the existing internal tablet radio. Often the radios of interest are Wi-Fi radios, but as described in section 3.1.3:*Open Source Radios* wide spectrum open source radios can be used for non 802.11 applications.

The most common means of tethering a radio to a tablet is via a USB cable. Frequently, there are options to tether either via the tablet's Bluetooth or Wi-Fi interfaces. However, the degree of interoperability is essentially the same, other than potential concerns about additional RF signals being emitted.

3.1.2.1.1 USB Wi-Fi Devices

Connecting an external device to a tablet via a USB cable is the most common connection type, and the only wired connection option[5]. The cable used is a USB OTG (On-The-Go) cable. Tablets are usually operated as a device connected to a host, but an OTG cable allows a device to connect to a tablet, with the tablet being the host. The tablet does have to support host mode and may have to have it enabled from within the OS settings.

Typically, the device connected to a tablet is an external USB Wi-Fi card that provides support for 802.11 communication protocols. This is used to replace the tablet's internal Wi-Fi with something with higher sensitivity and power. The device can have a replaceable antenna, so an antenna more suited to the user's requirements can be leveraged.

There are a large number of inexpensive USB Wi-Fi adaptors readily available. Because of the potential need to modify low-level protocols and radio operation, devices with open source drivers and preferably open source firmware are more appropriate for addressing the SA+C2 problem space. Furthermore, drivers that are integrated into the kernel are an even better option since enabling them is much simpler.

[5] Note that USB to Ethernet adaptors are another viable option if the radio of interest has an Ethernet connector.

Table 14:USB Wi-Fi Device Information

Documentation Set	Locations
An excellent source of information on the various Wi-Fi chips and open source driver support	http://wikidevi.com/wiki/Wireless_adapters/Chipset_table http://wireless.kernel.org/en/users/Drivers
Another resource for recommended Wi-Fi devices is to look for recommendation from the Wi-Fi developer community, whose members are especially interested in device capabilities	http://www.raymond.cc/blog/best-compatible-usb-wireless-adapter-for-backtrack-5-and-aircrack-ng/2/

Since it is envisioned that the networking devices are to be connected to an Android OS tablet and since Android OS does not have support for many drivers by default, connecting a device will require building in driver support for that device. This could be done either by enabling an integrated kernel, or by adding the driver to the kernel. The firmware needs to be installed into the device so it can be loaded by the driver.

Additionally, because MANET software requires the ability to leverage ad-hoc mode, any selected chip will need to provide ad-hoc mode driver support.

Another consideration is the power output of the Wi-Fi device. Several products provide an integrated solution with a Wi-Fi chip and a power amplifier with outputs of 500mW, 1000mW, and even as high as 2000mW. Such devices would achieve a longer range than standard devices at the cost of battery life.

Based on the various considerations there are several USB Wi-Fi products, shown in Table 15: *USB Wi-Fi Devices*, which are noteworthy.

Table 15: USB Wi-Fi Devices

Product	Description	References
Ralink RT5370	An inexpensive device available with open source drivers integrated into the kernel, but with a closed firmware configuration. Can be bought online for less than $10. The link is for the manufacturer information and downloadable driver sources.	http://www.mediatek.com/_en/01_products/04_pro.php?sn=1007 http://www.mediatek.com/_en/07_downloads/01_windows.php?sn=501
RealTek RTL8188	Another inexpensive product for less than $10. It has open source drivers integrated into the kernel and a closed firmware object.	http://www.realtek.com.tw/products/productsView.aspx?Langid=1&PFid=48&Level=5&Conn=4&ProdID=274 http://www.realtek.com.tw/downloads/downloadsView.aspx?Langid=1&PFid=48&Level=5&Conn=4&ProdID=274&DownTypeID=3&GetDown=false&Downloads=true
TP-Link TL-WN722N	A device readily available locally for about $20. It is based on the Atheros AR9271 chipset and works with the ath9k_htc driver. Unlike the previous two devices the AR9271 has open firmware, which potentially maximises the device's flexibility. An alternative to the TP-Link is the Alfa AWUS036NHA, which uses the same AR9271.	http://www.tp-link.com/CA/products/details/?model=TL-WN722N#spec http://wikidevi.com/wiki/TP-LINK_TL-WN722N http://wireless.kernel.org/en/users/Drivers/ath9k_htc https://github.com/qca/open-ath9k-htc-firmware
TP-Link TL-WN722ND	A higher power device (500mw) based on the Ralink RT3070, which has opens source drivers integrated into the kernel, but a closed firmware object.	http://www.tp-link.com/ca/products/details/?model=TL-WN7200ND http://wikidevi.com/wiki/TP-LINK_TL-WN7200ND
Alfa AWUS036H	The most recommend device for war-driving, provided 802.11n is not required. It has a rated output of 1000mW and is based on the Realtek RTL8187; the manufactures specifications are provided. A 2000mW version, Alfa, AWUS036H v2, is available now, however it is not getting good reviews due to its lack of stability.	http://www.alfa.com.tw/products_show.php?pc=34&ps=92 http://wikidevi.com/wiki/ALFA_Network_AWUS036H

3.1.2.1.2 Antennas

Antennas come in a wide variety of capabilities and ranges. For the purposes of this study there are two antenna types of interest:

1. 2.4GHz Wi-Fi antennas, and

2. Wideband antennas.

The first antenna type is intended for wireless Wi-Fi connections, increasing the range and sensitivity and possibly having directionality. The second type, the wideband antenna, is intended for more general applications; most likely used in open source radio applications and utilized in devices such as hackRF and bladeRF, as described in section 3.1.3:*Open Source Radios*.

Wi-Fi Antennas are either omni-directional or directional, the former being the most appropriate for indoor use and the latter common for outdoor and longer range communications. Omni-directional antennas are the simplest, smallest, and least expensive type of antenna. These are typically seen on USB Wi-Fi adaptors and wireless routers for indoor use. The antennas on routers and USB Wi-Fi devices are often 2dBi or 4dBi rated. However, they can be obtained with ratings of 5dBi and 8dBi. For example, TP-Link provides a range of antennas products, including:

- TL-ANT2405C: a 2.4GHz 5dBi Indoor Desktop Omni-Directional Antenna; and
- TL-ANT2408C: a 2.4GHz 8dBi Indoor Desktop Omni-Directional Antenna.

Directional antennas are most appropriately used outdoors, although indoor versions are available. Grid antennas can physically large (i.e., larger than a common satellite dish). Examples of many outdoor directional antennas can be found with up to 24dBi including:

- Tanszeo TR-GD24-24: a 2.4GHz 24 dBi Vertical/Horizontal Parabolic Wire Grid Antenna; and
- TP-Link TL-ANT24242B: 2.4GHz 24dBi Grid Parabolic Antenna.

These antennas can take high power input (100W) although radio for 802.11 will only provide a fraction of that power as input.

There are outdoor omni-directional antennas, although they appear to be less common. One example is from TP-Link:

- TL-ANT2415D: a 2.4GHz 15dBi Outdoor Omni-directional Antenna

Wideband Antennas become important for applications at frequencies other than 2.4GHz. These antennas offer coverage over a larger frequency spectrum, from 700 MHz to 11 GHz. Wideband antennas would be most appropriately used for an open source radio such as the bladeRF or hackRF.

Kent Electronics, the supplier of the antennas sold by Ettus Research for the USRP, offers a selection of inexpensive printed circuit board antennas. They require soldering of connectors or leads for connection to the radio, but are otherwise ready for use. Their products include log

periodic, Yagi antennas, and patch antennas among others. Their printed circuit board log periodic antennas come in three frequency ranges: 400-1000 MHz, 850-6500 MHz, and 2100-11000 Mhz.

Table 16: External Antenna Information

Manufacturer	Reference Material
Kent Electronics	http://www.wa5vjb.com/references.html http://www.wa5vjb.com/products.html Their printed circuit board log periodic: http://www.wa5vjb.com/pcb-pdfs/LogPerio400.pdf; http://www.wa5vjb.com/pcb-pdfs/LP8565.pdf http://www.wa5vjb.com/pcb-pdfs/LogPerio2000.pdf
Ettus Research	https://www.ettus.com/product/category/Antennas

3.1.2.1.3 Routers

Routers are an alternative to an external Wi-Fi device. Instead of using a simple wireless device, an entire router is connected to the tablet. Most likely the connection is via a USB to Ethernet adaptor, but a USB connection via an OTG cable is possible if the router supports USB. Some portable routers also offer WISP mode: Wireless Internet Service Provider to extend and boost Wi-Fi signals to devices when wireless signals are too weak for mobile devices alone. This is the network option proposed for architecture 2b, where access to the common networking mesh is made available to the display devices through the wireless routers.

In this arrangement the router is either simply an alternative means of connecting an external radio or it may take over some of the networking functions, including hosting the MANET. In the latter case the router would be modified from its standard firmware to a custom version with additional functionality. This requires installing one of the open source firmware suites for routers, such as OpenWrt. This firmware supports a large number of routers and the addition of software. If the device is to be used solely as a router, open firmware support may not be needed

Given the requirement for portability, a router that either includes a built in battery, or which can be powered by an external battery is preferred. Furthermore, a device with removable antennas that can be upgraded or connected to other equipment would be ideal. Unfortunately, routers sold for portability rarely have external antennas of any kind.

Given the requirements for portability and open firmware support there is a small selection of appropriate routers. The OpenWrt Wiki has a complete table of supported devices and hardware information. As noted previously, the Atheros chipsets have open drivers and open firmware, which provides the possibility of increased flexibility for low-level modification. The TP-Link

products feature Atheros Wi-Fi chips and they all use the same version of OpenWrt: target ar71xx. While an in-depth investigation of the capabilities of the many Wireless SoCs (System on a Chip) available was not part of this study, the availability of documentation led to a preference of open firmware solutions over SoC-based solutions.

For reference, the wireless options supported by OpenWrt firmwares are available at http://wiki.openwrt.org/doc/uci/wireless.

Table 17: Portable Routers

Router Provider	Locations
D-Link makes a portable router. While it is not supported by open firmware, it could still be useful if only standard router functionality is required.	http://www.dlink.com/ca/en/home-solutions/connect/routers/dir-506l-shareport-go
TP-Link makes portable routers with battery backup and support for open firmware. Devices include the TL-MR10U, and TL-MR3040.	http://wiki.openwrt.org/toh/tp-link/tl-mr10u http://www.tp-link.com/ca/products/details/?model=TL-MR3040#spec http://www.cnx-software.com/2013/09/29/27-tp-link-tl-mr10u-is-an-hackable-openwrt-wi-fi-router-with-a-power-bank/
TP-Link also has a version of the router that requires and external power supply.	http://www.tp-link.com/ca/products/details/?categoryid=218&model=TL-MR3020

3.1.2.1.4 MiniPCs

For increased flexibility beyond what is provided by an external router, a separate MiniPC can be deployed. In this scenario the external device is a complete PC, though a very small one, running a full Linux installation with multiple interfaces, including USB, Wi-Fi and Bluetooth.

The connection between the tablet and the MiniPC could use any of the interfaces according to the requirements. Since the MiniPC hosts a complete operating system, it could run the MANET software and be a member of the MANET, as a peer device, rather than being paired with a tablet. There are other options, such as installing sensor software, specialized protocols, network services, and wireless monitoring and reporting functions; the flexibility of these devices places few limitations on what can be achieved with the technology.

All MiniPCs include USB connectivity while some devices add wired networking, wireless networking, or Bluetooth. Because of the expandability, missing capabilities can be subsequently added. For example, a wireless USB device can be added to replace the baseline component to expand the features of the device or add a more powerful external antenna. For portability, the MiniPC could be battery powered by connecting to an external supply

MiniPCs are generally based on ARM processors. There are a limited few based on MIPS processors but they are uncommon and not well supported. This is in contrast to routers, where MIPS has a very strong presence and may even be dominant.

The MiniPC products can be divided into three categories of devices:

1. Smart TV – These are a class of MiniPC originally sold as Smart TV boxes, but they have since been adapted to run various Linux distributions;

2. Education boards – These are single board devices targeted to education and embedding, the best known being the Raspberry Pi; and

3. Development boards – These are the most powerful systems typically sold for embedded systems development.

Smart TV

Smart TV devices are inexpensive MiniPCs originally sold as Android Smart TV boxes and usually featuring a foreign manufactured SoC. Since their release, they have been modified by the open source development community to run full Linux distributions either as servers, desktop replacements, or multi-media boxes.

These products are sold with anywhere from 512MB to 2GB of RAM, and from 1 to 4 cores. They include USB (a host and an OTG connection), Wi-Fi and, in some devices, Bluetooth. They are sold in a case, with cables and power supply for less than $100. In many cases, they come with Android OS installed on an on-board flash, but there are aftermarket vendors with Linux preinstalled products. Notable SoC manufacturers include:

- Allwinner and Rockchip: The most common are from Allwinner and Rockchip, both ARM devices. These have become popular due to their very low cost and high performance.
- Freescale: An alternative are devices based on ARM-based Freescale processors. These are roughly double the price for less performance and so are less popular than other devices. A consequence of this is there is less community support, however Freescale does provide substantial amount of support documentation.

Allwinner MiniPCs were among the first devices to reach the North American market, beginning with the MK802 based on the single core A10 processor. Since then, devices based on the dual core A20 processor have been shipping. Linux support on these devices is very good with both Debian and Fedora being supported. Installation is a simple matter of copying an image to a micro SD card and booting the device; no flashing is required.

Rockchip MiniPCs are perhaps the most popular due to their high performance and low cost. The most popular are those based on the RK808 dual core processor and the RK3188 quad core

processor. Linux support for these devices has been developed by the community and is available by flashing the internal flash, or flashing a boot loader and kernel with a root on an SD card.

Mini PC models offered by these manufacturers are described below.

Table 18: Mini PC Manufacturer

Manufacturer / Model	Description	References
Allwinner MK802/ MK802 II	The MK802 was the first device and still one of the most popular; it has since been replaced by the MK802II with extra memory, and Bluetooth. The A20 quad core device is sold under the model QT800. Both devices are sold in many configurations.	Linux installations are available in several locations for the various distributions: https://www.miniand.com/forums/forums/2/topics/1 http://linux-sunxi.org/Bootable_OS_images
Rockchip MK808	The MK808 is very popular, as it has high performance processor (perhaps 4 times the power of a Raspberry Pi) with dual core processors running at 1.6 GHz and the cost is cost less than $50	Developer support and Linux support for the Rockchip product is provided by the community: http://www.rockchipfirmware.com/developer-tools http://ubuntu.g8.net/index.php/14-sample-data-articles/86-picuntu-4-5-nand-released
Freescale GK802	Freescale MiniPCs are much less common, the mode GK802 being the most common. Unfortunately installing Linux on the GK802 requires disassembly of the device. On the other hand, Freescale provides much better support with documentation and kernel sources.	Linux support for the GK802 is based on the Freescale kernel sources: http://www.linux.com/learn/tutorials/728212-how-to-install-linux-on-the-zealz-gk802-a-quad-core-a9-arm-on-a-stick

Education Boards

Education boards for programming and SoC development for the ARM processor have been popularized by the release of the Raspberry Pi board. Prior to its release there were other products for ARM development but they were much more expensive. A Raspberry Pi board can be bought for $35, and a complete system for $70 (including power supply, case, and SD card).

Since the Raspberry Pi was released, other products have been introduced for similar markets, such as the BeagleBone Black, offering an alternate set of features. An advantage of these boards is their extreme flexibility, with lots of connections, active community support, and the availability of assorted hardware options.

Raspberry Pi is an inexpensive board originally aimed at the education market. It has become very popular due to its low price, easy availability globally, and active developer community.

The device has a 700MHz ARM processor, 512MB of RAM, 2 USB ports, a micro USB power connector, HDMI output, composite video output, analogue audio output, Ethernet connector, and an SD card slot. It has two sets of GPIO pins for adding extra daughter boards. The SD card functions as both boot device and storage.

The BeagleBone Black is similar to the Raspberry Pi with slightly better specifications. Like the Raspberry Pi it is aimed at the education, and developer community. The BeagleBone Black is a $45 device with a 1GHz ARM Cortex-A8 process, 512MB of ram, 2GB of eMMC on-board-flash, 2 USB ports (host and client) Ethernet, HDMI, and GPIO pins. It runs Android OS and several Linux distributions.

Additional information regarding education boards can be found at the following locations.

Table 19: Raspberry Pi Information

Documentation Set	Locations
A list of Linux distributions available for the Raspberry Pi.	http://www.raspberrypi.org/downloads
The Raspberry Pi does not have a real time clock, but one can be added	http://afterthoughtsoftware.com/products/rasclock
Clock Synchronization solutions for the Raspberry Pi.	http://www.satsignal.eu/ntp/Raspberry-Pi-NTP.html
Most notably, the Raspberry Pi is shown powering and bladeRF open source radio	http://nuand.com/

Development Boards

Development boards for the ARM processor offer a more capable platform for ARM development by providing larger amounts of RAM and faster processors. Typically they are targeted to developers who need more performance and are unable to use a cross platform environment. They come at a higher cost, over $100, but less that $200 (although there are more expensive options), and are based on chipsets providing more documentation and support.

Only two development boards are listed here since they are less relevant to this study as compared to the devices described earlier in this section. Development boards are more expensive and are targeted for a specific market as opposed to boards such as the Raspberry Pi which is low cost and general purpose serving a broader community.

1. ODROID-U2 is a compact device based on the Samsung Exynos 4412 Prime, 1.17GHz ARMS Cortex-A9 quad core processor. It features Ethernet, 2x USB ports, audio, power connectors, micro HDMI, and micro SD. The device supports both Android and Linux and has significant community support.

2. ODROID-XU is a compact device based on the Samsung Exynos 5 Octa. This is a Cortex A15 1.6 GHz quad core and a Cortex A7 quad core, for a total of 8 ARM cores. It features Ethernet, 3x USB ports (1x 3.0), audio, power connectors, micro HDMI, and eMMC 4.5 flash storage. The device supports both Android OS and Linux.

3.1.2.2 Tablet Integrated Solutions

As an alternative to an external radio, the tablet itself can be an active part of the solution via its own integrated radio. Tablets have up to 3 different on-board radios: an 802.11 wireless radio, a Bluetooth radio, and for 3G enabled devices, a cellular 3G radio.

For MANET applications it is the 802.11 Wi-Fi radio that is of interest. Because tablets are sealed units, whatever radio and antenna is part of the tablet is the only option for that tablet. For anything else either an external device has to be configured, or the tablet has to be physically opened, violating any product warranty (and likely making the product less robust).

DRDC-directed research that preceded this investigation configured a MANET solution based on the Lenovo Ideapad A1. This is a single core 1GHz Cortex A8 with 512MB of RAM, 2GB of internal memory, and supports both 802.11b/gn and Bluetooth 2.1.

When considering alternative tablets for the MANET development it is worth looking at the requirements for the MANET Manger software, as defined at the Google Play Store:

1. Root access to the device

2. Kernel which supports wireless extensions (*wext*)

3. Wireless device driver which supports ad-hoc mode

There is a list of supported devices, some needing custom kernels:

- Samsung Galaxy Tab 10.1
- Samsung Galaxy S II Epic Touch 4G SPH-D710
- Samsung Galaxy Nexus SCH-I515 (custom kernel)
- Samsung Galaxy S III GT-I9300 I9300UBDLJ1 (Latin American countries) (custom kernel)
- Samsung Galaxy S III GT-I9300 I9300XXBLH1 (Nordic countries) (custom kernel)
- ASUS Transformer Prime TF201 (custom kernel)
- ASUS Nexus 7 / Google Nexus 7 (custom kernel)

The Nexus 7 is most interesting because of its excellent support over many updates to the Android OS. (This device is often referred to as the Google Nexus 7.)

As part of this study, a Nexus 7 was used to successfully run and launch the MANET Manager software. This required updating the firmware with a kernel supporting ad-hoc mode. Rather than use the MANET Manager custom kernel, the latest version from Cyanogenmod[6] was installed. The versions starting from 10.2 have fully integrated support for ad-hoc-networks. In a separate test, the Nexus 7 was able to utilize an external USB wireless card, the TP-Link TL-WN722N using a custom kernel with driver support A newer version of the Nexus 7, version 2013, has been released and it is expected to have the same degree of support from Cyanogenmod and be capable of running MANET Manager.

Table 20: Android Tablet Information

Documentation Set	**Locations**
Lenovo Tablet Specifications	http://shopap.lenovo.com/ISS_Static/WW/ap/in/en/merchandising/sitelets/Lenovo-A1-Tablet/PDF/Lenovo-IdeaPad-A1-datasheet.pdf
Technical Specifications for the Nexus 7 tablet	http://www.google.ca/nexus/7/specs/
Integrated Support for ad-hoc networking on the Nexus 7 tablet	http://wiki.cyanogenmod.org/w/Grouper_Info
TP-Link TL-WN722N support using a custom kernel with driver support	http://forum.xda-developers.com/showthread.php?t=2240845 http://forum.xda-developers.com/showthread.php?t=2240845&page=4

Mentioned in the above links is the deployment of a Kali, a Linux-based operating system that hosts a suite of vulnerability assessment tools within a software jail. This is a topic that is covered in more detail in section 3.1.4.2: Kali Linux and section 4.2.1:*Co-Existence and Isolation of Code on Android Devices*.

[6] Cyanogenmod, an open source operating system for tablet architectures that is based on the Android mobile platform, is discussed in more detail in 3.3.1:*Tablet-based MANET Configuration*.

3.1.3 Open Source Radios

Open Source Radios provide significant access to the device and software for modification to the radio to support new applications. These radios may have open source software support, open hardware, or open designs. In the case of one radio, the HackRF, the radio design, the components, and software are all freely accessible.

Many of the open source radios investigated in this study are supported by GNU Radio, an open source project for the design and implementation of Software Defined Radios (SDR). GNU Radio software permits the design of radios by flow diagrams using the Python programming language. A GUI extension, GNU Radio Companion, provides a graphical tool for radio design based on components such as filters and modulators.

One of the first open source SDRs with GNU Radio support is the USRP from Ettus. In the last year, two other products have arrived or will arrive shortly, the bladeRF from Nuand and the HackRF from Great Scott Gadgets. Another interesting device is the RTS-SDR, a very inexpensive device (less than $20) that was originally sold as a TV tuner, but has since become popular as a receive-only SDR with a variety of applications.

In this section the above devices will be presented, along with brief mention of several other potentially interesting products.

3.1.3.1 Great Scott Gadgets HackRF

Table 21: HackRF Specifications

Product Type	Software Defined radio	
Product Features	HackRF is an open source hardware project to build a Software Defined Radio (SDR) peripheral. HackRF operates from 30 MHz to 6 GHz, a wider range than any SDR peripheral available. This range includes the frequencies used by most digital radio systems. It can operate at even lower frequencies in the MF and HF bands when paired with the Ham It Up RF upconverter. HackRF can be used to transmit or receive radio signals. It operates in half-duplex mode: it can transmit or receive but can’t do both at the same time. However, full-duplex operation is possible if you use two HackRF devices. The device is powered by the USB connection to a host and is intended to be portable.	
Specifications	Range	Short range
	Frequency	30 MHZ – 6 GHz
	Bandwidth	20 MHz
	Power	5 dBm to 15 dBm
	Sample	8 bit / 20 Msps

	Size/rate	
	Additional	USB 2.0 interface
	Price	$300
Project Sources	The project web page	http://greatscottgadgets.com/HackRF
	Hardware design and software	https://github.com/mossmann/HackRF
	Project documentation	https://github.com/mossmann/HackRF/wiki
	Interviews and blogs with the HackRF developer	http://www.theamphour.com/the-amp-hour-161-gifted-grimgribber-grokker/ http://ossmann.blogspot.ca/search/label/HackRF http://hak5.org/episodes/hak5-1120

The most important aspect of HackRF is its open source design: all hardware designs and software source code is available under an open source licence. The interface is a standard USB 2.0 for both power and signal, and it is supported by GNU Radio software.

The first HackRF was completed at the end of November 2013. Its design is a result of the lessons learned from a beta board known as JawBreaker that was delivered to 500 developers with funding assistance from DARPA.

3.1.3.2 Nuand bladeRF

Table 22:bladeRF Specifications

Product Type	Software Defined radio	
Product Features	bladeRF is a Software Defined Radio (SDR) built for both the radio enthusiast community and professional radio engineers for exploration and experimentation into RF communication. Source code and documentation are provided with the product to demystify SDR concepts including hardware, firmware and device drivers. bladeRF is focused on education and includes a set of tutorials. The bladeRF is powered by the USB 3.0 interface. The same connection can be used for host processing. It can also be used standalone, powered by 5V DC and using the onboard FPGA for signal processing. An FPGA programming option (a header with switches and lights) turns the bladeRF into an FPGA development board.	
Specifications	Distance	Short range
	Spectrum	300MHz to 3.8GHz
	Bandwidth	28 MHz
	Sample Size/rate	12 bit/40 Msps
	Additional	USB 3.0 interface Full Duplex
	Price	$450
Project Sources	The project web page	http://www.nuand.com
	Hardware design and software	https://github.com/mossmann/HackRF
	Products and ordering	http://www.nuand.com/blog/shop/
	Project support	http://www.nuand.com/support.php

The bladeRF SDR tunes from 300MHz to 3.8GHz and can be used immediately with GNU Radio drivers. Not only is the host software open source, the USB 3.0 microcontroller (Cypress FX3) is available, as is the Field Programmable Gate Array (FPGA) Very High Speed Integrated Circuit (VHSIC) Hardware Description Language (Altera Cyclone IV), thus giving extra development

flexibility. Reprogramming can be accomplished either via Joint Test Action Group (JTAG) or via USB using tools provided by the hardware vendors.

bladeRF is currently commercially available. Besides the main board there is a General Purpose Input Output (GPIO) expansion board for FPGA development, and an HF/VHF transverter that made the bladeRF suitable for HF/VHF application by extending the frequency down as low as 10MHz (high fidelity down to 50MHz).

3.1.3.3 ETTUS USRP B200/B210

Table 23: Ettus radio Specifications

Product Type	Software Defined radio	
Product Features	The Ettus USRP is one of the original affordable Software Defined radios. They have a long history of involvement with the GNU Radio project and their products have GNU Radio support. The newest products (2013-08-22), the USRP B200 and USRP B210 are the first devices from Ettus that are fully integrated with RF coverage from 70MHz to 6 Ghz. (Previous devices from Ettus require daughter boards for each of the frequency ranges covered.)	
Specifications	Distance	Short range
	Spectrum	50 MHZ – 6 GHz
	Bandwidth	56 MHz
	Sample Size/rate	12 bit / 56 Msps
	Additional	USB 3.0 interface Full Duplex
	Price	$780 motherboard / $90 basic daughterboard
Project Sources	Company web page	http://ettus.com
	Blog and background	http://www.ettus.com/blog
	Product support	http://www.ettus.com/support

The B200 and B210 transceivers have up to 56MHz of bandwidth, and reprogramming FPGA (Spartan6) and USB 3.0 interface. A standard Universal Software Radio Peripheral (USRP) Hardware Driver (UHD) allows both devices immediate support via GNU Radio. One of the primary differences between the two models is support for dual channel Multiple Input/Multiple Output (MIMO).

3.1.3.4 RTL-SDR DVB-T

Table 24: RL-SDR DVB-T Specifications

Product Type	Software Defined radio	
Product Features	The RTL-SDR is a TV tuner dongle based on the Realtek RTL2832U. It can be used as a cheap SDR (Software Defined Radio) since the chip allows processing of the raw digital samples.	
Specifications	Distance	Short range
	Frequency / Bandwidth Sample Size/rate	See below
	Price	$20
Project Sources	Device information	http://sdr.osmocom.org/trac/wiki/rtl-sdr
	Product background	http://rtlsdr.org
	How to use RTL-SDR to crack GSM phone calls	http://hackaday.com/2013/10/22/cracking-gsm-with-rtl-sdr-for-thirty-dollars
	Raspberry Pi for short range, low bandwidth wireless	http://hackaday.com/2013/11/09/transmitting-data-with-a-pi-and-rtl-sdr

The RTL2832U outputs 8-bit raw signal samples, and the highest theoretically possible sample-rate is 3.2 MS/s; however, the highest sample-rate without lost samples that has been tested so far is 2.4 MS/s. These numbers vary between the various versions of the chipset. Table 25: *RTL2823U Chipsets and Associated Frequency Ranges* gives a list of available chipsets for the RTL2823U SDR.

Table 25: RTL2823U Chipsets and Associated Frequency Ranges

Chipset	Frequency Range
Elonics E4000	52 - 2200 MHz with a gap from 1100 MHz to 1250 MHz (varies)
Rafael Micro R820T	24 - 1766 MHz
Fitipower FC0013	22 - 1100 MHz (FC0013B/C, FC0013G has a separate L-band input, which is unconnected on most sticks)
Fitipower FC0012	22 - 948.6 MHz
FCI FC2580	146 - 308 MHz and 438 - 924 MHz (gap in between)

The RTL-SDR device is support by GNU Radio and a large number of third party applications. Although the RTL-SDR is "receive only", there have been hacks marrying this device with a Raspberry Pi, using the Raspberry Pi to transmit and the RTL-DSR to receive short-range communications.

3.1.3.5 Additional Open Source Radios

Besides the devices described above, there are several other products on the market. Some of these are detailed in the Table below.

Open Source Radio	Resource Information
Agile Solutions ASRP – Agile Solutions has 2 versions of the ASRP, the ASRP1 and ASRP3. The ASRP3 is a wideband receiver in a USB form factor with a range of 400MHz to 4.4.GHz. The ASRP1 is a full duplex MIMO SDR system. It features an Altera Cyclone FPGA and a Cypress FX2 USB.	http://agile-sdr-solutions.com/ASRP3 http://agile-sdr-solutions.com/ASRP1.
Myriad-RF – Myriad is an open source wireless platform RF module, it is not a complete SDR peripheral access 260MHz through 3.8 Ghz. The board is based on an open source reference design A comparison to the HackRF SDR is provided.	http://myriadrf.org/myria-rf-board-1 http://dangerousprototypes.com/2013/03/13/myriad-rf-open-source-wireless-platform/
Fairwaves – The UmTRX v2.1 is an SDR transceiver with a 1GbE Ethernet connection similar to the Ettus USRP N series. It has two full duplex transceivers processing 300MHz to 3.8GHz, and features a Spartan 6 FPGA.	http://umtrx.osmocom.org/trac/.

3.1.3.6 Comparing Open Source Radios

The three radios that are of most interest, because of their price and expected availability, are the HackRF, the bladeRF, and the USRP B200. The RTL-SDR is interesting because of its extremely low cost (less than $20), but is a "receive only" device, while the ASRP3, MyiadRF and the UmTRX lack the popularity and community support of the other devices.

Both the bladeRF and the USRP B200 are shipping, now while the HackRF is expected to ship in February 2014. The HackRF appears to be generating a lot of interest in the SDR community, because of its relatively low cost compared to earlier products. It has gotten the attention of DARPA who have funded the project to build a beta board (JawBreaker) and distribute 500 units free to interested developers. Both bladeRF and HackRF were Kickstarter funded projects.

The Ettus B200 and B210 are new products from Ettus. They differ from their earlier offerings in that they are a single board solution, compared to their earlier products that required the addition of daughter boards to cover various portions of the RF spectrum.

A detailed comparison of the radios is provided below[7].

<table>
<tr><th rowspan="2"></th><th rowspan="2">HackRF</th><th colspan="2">bladeRF</th><th colspan="3">USRP</th></tr>
<tr><th>x40</th><th>x115</th><th>B100 Starter</th><th>B200</th><th>B210</th></tr>
<tr><td>Radio Spectrum</td><td>30 MHz – 6 GHz</td><td colspan="2">300 MHz – 3.8 GHz</td><td>50 MHz – 2.2 GHz [1]</td><td colspan="2">50MHz – 6 GHz</td></tr>
<tr><td>Bandwidth</td><td>20 MHz</td><td colspan="2">28 MHz</td><td>16 MHz [2]</td><td colspan="2">61.44 MHz [3]</td></tr>
<tr><td>Duplex</td><td>Half</td><td colspan="2">Full</td><td>Full</td><td>Full</td><td>2x2 MIMO</td></tr>
<tr><td>Sample Size (ADC/DAC)</td><td>8 bit</td><td colspan="2">12 bit</td><td>12 bit / 14 bit</td><td colspan="2">12 bit</td></tr>
<tr><td>Sample Rate (ADC/DAC)</td><td>20 Msps</td><td colspan="2">40 Msps</td><td>64 Msps / 128 Msps</td><td colspan="2">61.44 Msps</td></tr>
<tr><td>Interface (Speed)</td><td>USB 2 HS (480 megabit)</td><td colspan="2">USB 3 (5 gigabit)</td><td>USB 2 HS (480 megabit)</td><td colspan="2">USB 3 (5 gigabit)</td></tr>
<tr><td>FPGA Logic Elements</td><td>[4]</td><td>40k</td><td>115k</td><td>25k</td><td>75k</td><td>150k</td></tr>
<tr><td>Microcontroller</td><td>LPC43XX</td><td colspan="2">Cypress FX3</td><td>Cypress FX2</td><td colspan="2">Cypress FX3</td></tr>
<tr><td>Open Source</td><td>Everything</td><td colspan="2">HDL + Code Schematics</td><td>HDL + Code Schematics</td><td colspan="2">Host Code [5]</td></tr>
<tr><td>Availability</td><td>January 2014</td><td colspan="2">Now</td><td>Now</td><td colspan="2">Now</td></tr>
<tr><td>Cost</td><td>$300 [6]</td><td>$420</td><td>$650</td><td>$675</td><td>$675</td><td>$1100</td></tr>
</table>

[1] – Separate daughterboards are required to receive/transmit. The WBX transceiver is included in this kit
[2] – Half this if 16 bit samples are used
[3] – 56 MHz for single half duplex channel, 30.72 MHz per channel full duplex
[4] – There is a CPLD on the board, but no FPGA
[5] – Ettus confirmed that the HDL + Code + Schematics will be released for the B210/B200
[6] - Estimated retail price, cheaper though Kickstarter

Both the bladeRF and HackRF boards have options boards that can extend the frequency coverage downwards. The bladeRF add-on is the HF/VHF transverter and it extends the

[7] With acknowledgement to Taylor Killian (http://www.taylorkillian.com/2013/08/sdr-showdown-HackRF-vs-bladerf-vs-usrp.html)

frequency down to 50MHz and even down to 10MHz if high fidelity is not required. The HackRF add-on is the Ham it Up converter that extends the frequency coverage down to 300KHZ. The limit on the upper end of the bladeRF frequency means it is unable to see traffic in the 802.11n 5GHz band, while both the other devices do cover 5GHz.

A limitation of the HackRF is that it is half duplex, so it is either receiving or transmitting and has to be switched from one to the other. Both the bladeRF and the USPR are full duplex. Community experience with these devices indicated that there may be issues with full duplex causing interference due to the close proximity of the radio components. Interference may also be an issue using USB 3.0 at high speed.

All of the devices have powerful onboard processors; they are not just RF boards. The USRP and bladeRF have on board FPGA, while the HackRF does not. The FPGAs can perform processing on-board and thus reduce the data transferred to the host computer, and there is space for user additions to the FPGA. For example, this has been used to improve the performance of the BBN Technologies 802.11 implementation in GNU Radio, as discussed in the following section. Besides the FPGAs, all the devices have on board ARM microcontrollers that deal with the radio and USB interface and are user programmable. The extra processing on the bladeRF and USRP means they can be run headless (without a host computer) for some applications.

A difference between the SDRs is the openness of the hardware and software. All of the boards are supported by GNU Radio, and the drivers are part of the distribution. The code and schematics are available as well, but HackRF even makes the design files available so it is possible to build your own HackRF, or to change the design and build your own version. An empty board can be purchased and there are directions provided for assembling your own device. HackRF also prides itself on using only hardware for which design info has been releases without an NDA.

3.1.4 Open Source SDR Support

This section presents a discussion of open source and open architecture SDR hardware and radio-based software projects that have a relevance to the envisioned SA+C2 mobile device.

3.1.4.1 GNU Radio

GNU Radio is free software toolkit for developing building blocks to implement software radios.. It performs signal processing in the physical layer with a range of commercially available RF equipment such as bladeRF, HackRF, Ettus USRP, and the Realtek RTL-SDR dongles.

Applications are written in Python describing a flow graph of interconnected signal processing blocks coded in C++. A developer who understands the fundamentals of radio and signal processing can deal with a wide range of RF processing in GNU Radio. GNU Radio Companion is a graphical interface for the development of GNU Radio applications.

There is a wide range of technical articles and supporting documentation for GNU Radio. The following references are deemed to be a thorough representation of the technology across a broad set of capabilities.

Table 26: GNURadio Reference Documentation Set

Documentation Set	Locations
Tutorials, installation instructions and primers for the technology (the main GnuRadio site)	http://gnuradio.org/redmine/projects/gnuradio/wiki
How to use GNU Radio and the GNU Radio companion	http://gnuradio.org/redmine/projects/gnuradio/wiki/HowToUse http://gnuradio.org/redmine/projects/gnuradio/wiki/GNURadioCompanion
Set of tutorials on GNU Radio from Ettus	http://www.ettus.com/kb/detail/software-defined-radio-usrp-and-gnu-radio-tutorial-set
GNU Radio drivers for the bladeRF, HackRF and RTL-SDR, with some examples	http://sdr.osmocom.org/trac/wiki/GrOsmoSDR
An in depth article on data transmission bandwidth with GNU Radio and the USRP	http://www.wu.ece.ufl.edu/projects/wirelessVideo/project/GNU_Radio_USRP
The BBN Technologies 802.11b receiver and transmitter for GNU Radio. The project implements a basic 802.11 transmitter and receiver, which is able to decode low rate 802.11 packets from standard NICs over the air reliably at 1Mbps and partially at 2Mbps	https://www.cgran.org/wiki/BBN8021
A research project to extend the 802.11 work with BBN and GnuRadio that reduces the USB data transfer requirements by programming the FPGA of an USRP to implement full-rate dispreading. This implementation achieves 2Mbps with a reception range of 20 meters	http://span.ece.utah.edu/pmwiki/pmwiki.php?n=Main.80211bReceiver
This project implements GPS using GNU Radio. GNSS-SDR is an open-source Global Navigation Satellite System software defined receiver that provides a common framework for GNSS signal processing	http://gnss-sdr.org/documentation/gnss-sdr-operation-realtek-rtl2832u-usb-dongle-dvb-t-receiver https://www.cgran.org/wiki/gnss-sdr http://gnss-sdr.org/

3.1.4.2 Kali Linux

Kali Linux is a Linux distribution and LiveCD for penetration testing, derived from the earlier and well known BackTrack distribution. While it includes many tools for penetration testing, of most interest are those used for wireless development and managing SDRs.

The SDR additions are recent and have only been added in the most recent release (1.0.5). Most notably are tools for supporting the RTL-SDR device, including testing, scanning, AM and FM radio, and GNU Radio. This includes the gr-osmosdr driver for support of both the RTL-SDR device, HackRF/bladeRF, and UHD for the USRP. GNU Radio and GNU Radio Companion are included and updated to the latest versions.

Table 27: KALI Linux Reference Documentation Set

Documentation Set	**Locations**
The main site for Kali Linux including download and support	http://www.kali.org/
Plans for extending Kali support for SDR	http://www.kali.org/news/kali-linux-software-defined-radio-support
Kali Linux can be installed on a number of ARM devices including the Raspberry Pi	http://docs.kali.org/armel-armhf/install-kali-linux-arm-raspberry-pi

3.2 Tablet Component

Another key component of the proposed architectures is the tablet display device. For both military and commercial offerings (e.g., TrellisWare and Persistent Systems), these are typically Android OS devices providing a high quality touch display, a USB interface, camera, microphone, speakers, GPS, Bluetooth, Wi-Fi networking, motion sensors, and integrated battery. Although they contain a broad set of inherent capabilities, they generally lack the ability to upgrade components or alter the internal hardware configuration.

3.2.1 Tablet Configurations

Tablets are available in a wide variety of sizes between 4 and 10 inches, but the most common form factors are 7 and 10 inches. There are limited controls, with almost everything controlled through the touch screen; however, there is a power button, and volume buttons, which do double duty for resetting the device and dealing with boot loader and recovery functions.

The key components of any tablet are the memory and the CPU (including an integrated GPU). System memory consists of a flash memory device for holding the OS, file system, and RAM for processing.

Tablets have a range of flash sizes—usually 16GB or 32GB, although 8GB is available but is becoming less common, and 64GB is still uncommon. RAM size is 512MB to 2GB with 1GB being the most common and 2GB becoming more common. The ARM processor in most tablets has a maximum RAM capacity of 2GB, so high capacities will not be seen until the next generation or on tablets not based on the ARM processor.

Android tablets are typically based on some version of the ARM processor. Early versions were single core; now most tablets are at least dual core and increasingly they are quad core, with 8 core versions expected at some point in 2014. There are Android tablets based on MIPS processors, but they are targeted towards the lower end market since the less expensive processor allows the device to retail more cheaply. The MIPS processor also uses less power, so batteries are correspondingly smaller and cheaper. However, it is significant to note that not all Apps for Android are supported on MIPS processors.

Tablets have an integrated rechargeable battery that is generally intended to last one day of regular use, but this is highly dependent on what is being done with the tablet. For example, watching HD video or running the Wi-Fi connection can dramatically shorten battery life to a few hours. If more power is needed, either the device has to be plugged into an outlet, or an external battery.

3.2.2 Tablets and Radio Configuration

This section examines the tablet and radio configuration from the perspective of the tablet device. When examining the relationship between the tablet device and the radio that will be used to join the device to the SA+C2 tactical MANET, there are two options that are available:

1. Use of the internal radio that is integrated with tablet to connect to the MANET, or

2. Use of an external radio connected to the tablet to connect to the MANET.

3.2.2.1 Internal Radios

In evaluating the first option there are clear advantages and disadvantages to the use of the integrated radio. An internal Wi-Fi radio is included with all Android tablet configurations and is therefore a communications component that will be both available and compatible with the tablet. However, in keeping with the target market for tablets (home/business user) the radios that are provided with tablets are generally low power components and are range limited by the small internal antenna. Long range communication using tablets is not a needed capability for the typical user and in the competitive tablet market space the use of low power components is seen by the manufacturer as a means to stay price competitive. Similarly, no tablets have been found that allow replacing the internal antenna with an external one without performing a hardware modification to the tablet device. While power and range is one significant factor in the selection of the main radio component for the SA+C2 device, openness is another factor where internal radios are at a disadvantage. Internal Wi-Fi radios use radios (such as the Broadcom chipset) that are much less open in terms of architectural documentation and available source code as compared to radios that are not bound to the tablet architecture, such as Atheros based chips.

3.2.2.2 External Radios

When examining the second option, namely radios that are not integrated with the tablet hardware and are accessed externally, it is evident that the disadvantages seen with internal radios are mitigated. Three types of external radios are applicable to this space.

1. <u>External Wi-Fi Radios</u>: An external Wi-Fi radio can be selected for the SA+C2 device where the radio's Wi-Fi chipset includes the needed features and capabilities. As a result, the selection of the tablet and the selection of the radio become two separate decisions with the opportunity to choose the best component for the task in each case. Additionally, the selection of external radio can ensure that the radio's drivers, firmware and architecture are all fully open and published. This will allow the radio's behaviour to be configured and modified to suit the requirements of the SA+C2 device and applications. The radio can also be chosen for its support of power amplifiers and external antennas. Hardware from Atheros, for example, has both open drivers and open firmware, increasing the possibility of making changes to the radio. Some products have integrated amplifiers (which unfortunately increases the power consumption) to get greater range. Finally antennas can be selected in a variety of gains or can be unidirectional to increase the range even further.

2. <u>Commercial Broad Spectrum Radios</u>: External radios with MANET support can be leveraged to support communications with protocols other than Wi-Fi and to offload the MANET requirements from the tablet. Commercial vendors such as Persistent Systems and TrellisWare Technologies have optimized the hardware and software of their radios for MANET support. While these products provide high performance, optimized protocol support and architectural rigor, the cost per unit is significantly higher. Additionally, the interface specification presented by the radio to a tablet device will be: limited, not fully open and subject to change by the manufacturer. This poses a restriction on the type of SA applications that could be developed for the SA+C2 device without assistance from the manufacturer of the radio. For example, both Persistent Systems and TrellisWare

Technologies have APIs for their radios, but they are not publicly available. Obtaining them requires either to become a customer or perhaps to sign an NDA.

3. Open Architecture Radios: Devices such as bladeRF and HackRF supply a fully documented open design and open source drivers and applications. Using applications such as GNU Radio one can (theoretically) construct a myriad of radios and protocols. As such, application development for SA tools can be done with fewer restrictions and greater support. Leveraging the capabilities of an open radio can only be realized once basic connectivity is achieved between the tablet and the radio; a more significant challenge as compared with the other radio types. At a minimum, utilizing open radios would require hosting the appropriate software (e.g. GNU Radio) on either:

   a. the tablet; or

   b. an external computing device (e.g., a miniPC or Raspberry Pi) connected to both the radio and the tablet.

   Getting GNU Radio to run on a tablet device may be feasible since there is Linux support for the software. There will still be a hardware/software integration effort to allow the three components—tablet, radio and GNU Radio software—to operate successfully.

   Using an external computing device to control the open radio would mitigate some of the uncertainty in this integration effort but adds complexity to the overall solution architecture. A proposed configuration would separate the interfaces between components: applications would be developed for the computing device and the tablet would access these applications through a defined interface.

3.2.2.3 MANET Support for Radios

The Android tablet internal radio is supported by the MANET Manager application; however, the tablet device must be configured to support ad-hoc mode which is not typically part of the Android build configuration. There are kernel patches to enable ad-hoc mode and the latest version of Cynogenmod (10.2) includes ad-hoc as part of the standard build configuration. In this scenario the MANET would be established by the tablet regardless of whether the internal or an external Wi-Fi radio is being used. In either case, the radio is accessed and controlled by the same Wi-Fi software:

- *wpa_supplicaint* for managing connections, and
- *iwmulticall* for device control,

It is significant to note that different device drivers will be used to access the radio itself and as such, some radio features may not be supported on all Wi-Fi chips.

Application development for the tablet/radio combination would be done by using the Android development kit. Apps are built to use the tablet touch display and can access the Wi-Fi networking subsystem. Applications might be general applications such as plotting location or radio specific such as reporting signal strength and packet errors. There are several Apps, available through Google Play, that would be useful on an Android device with a Wi-Fi radio:

- **Fing Network Tools** for general network management

- **Network Status** to acquire details of the network connection
- **My Location** provides current latitude, longitude and maps current location;
- **WiFi Manager** shows status of the Wi-Fi, signal quality, errors, bandwidth;

3.3 MANET Implementation

While the previous sections have examined the tablet and radio elements of the SA+C2 device architecture, it must be emphasised that the design goal for the device is to participate in a MANET in order to exchange SA information with members of the tactical unit. The device must host applications that will support the sharing of C2 within a closed community of dismounted soldiers in the field. As such, the MANET that is configured to provide the flexibility, security and robustness in the tactical mesh network is as essential a component as the handheld and communications devices that will comprise the SA+C2 device.

The MANET is established and maintained by a combination of hardware and software elements. For the discussion in this section, these elements are broken down into two separate approaches:

1. **Tablet-based MANETs** where the MANET support is provided by the handheld; and

2. **Radio-based MANETs** where the MANET participation is provided by the radio.

3.3.1 Tablet-based MANET Configuration

As shown in Figure 14: *A Tablet-Based MANET*, in a tablet based MANET configuration the responsibility for joining and participating in a MANET is a function performed by the tablet OS, network drivers and supporting applications hosted at the tablet. The logical boundary of the MANET is extended to the tablet OS and the radios (internal or external) simply serve to exchange radio signal information between other radios in the environment. The radios have no knowledge of the MANET protocol or that a MANET is in place at all.

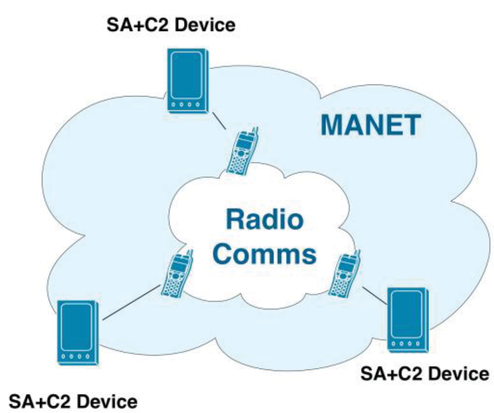

Figure 14: A Tablet-Based MANET

The necessary software to establish a tablet-based MANET is available from the Google Play Store.

Table 28: MANET Software for Android Devices

Application	Locations
MANET Manager: An App for starting and controlling a MANET service running on a tablet	https://play.google.com/store/apps/details?id=org.span&hl=en
MANET Visualizer: An App for showing the devices interconnected by the MANET	https://play.google.com/store/apps/details?id=org.span.visualizer&hl=en
MANET Voice Chat: An App for a push-to-talk service on a MANET connected tablet	https://play.google.com/store/apps/details?id=org.span.ptt&hl=en

In order to use this software, the tablet running the MANET service requires root access, a kernel with wireless extensions, and a Wi-Fi device that support ad-hoc mode. For example, one of the devices supported by the MANET Manager app is the ASUS Nexus 7 with a custom kernel that is supplied by the developers. Furthermore the latest versions of Cynogenmod (10.2) have added full support for ad-hoc mode, thus the MANET App is inherently supported.

NOTE: During this effort The MANET Manager app was successfully installed and run on a Nexus 7 2012 support by an installation of Cynogenmod 10.2 Nightly build.

The Google Play Store has the following description of the MANET Manager App:

> *This simple app allows you to enable and configure a Mobile Ad-Hoc Network (MANET) for your device. Install the app on another device and they will automagically recognize and link to each other when they are within ~500 feet. Install the app on even more devices and expand the range of your mesh network! The app will route data from one device to another and "hop" across other devices in the mesh to get there. In short, the more devices in your mesh the greater your communications range.*

Interestingly, this app also allows you to share your phone's cell connection with other devices in the mesh network. Support for the App is available in a Google Group and the source code is available for knowledge transfer and modification subject to licensing restrictions. MANET Manager is an active project; prior work by DRDC found that the development team for MANET Manager was responsive to questions and comments.

The MANET Manger is an App relying on an underlying MANET routing protocol using the OLSR daemon (OSLRd), which is an implementation of the Optimized Link State Routing Protocol. The daemon is portable and runs on most platforms, including Linux, Android, Windows, and OS X. It is fast and uses very little CPU and thus is suited to low power embedded devices.

The OLSR daemon is implemented using the OLSRd open source software package. The OLSRd site contains the following description of the software:

> *OLSR is a routing protocol for mobile ad-hoc networks. The protocol is pro-active, table driven and utilizes a technique called multipoint relaying for optimized message flooding. olsrd also implements a popular optional link quality extension.*
>
> *Olsrd is meant to be a well-structured and well coded implementation that should be easy to maintain, expand and port to other platforms. It has a very flexible plugin architecture.*
>
> *The implementation is RFC3626 compliant with respect to both core and auxiliary functioning.*
>
> *Olsrd supports use of loadable plugins. These can be used to to handle and generate custom packet types to be carried by OLSRs MPR flooding scheme or for any other desired functioning.*

The following references provide more in-depth information regarding ad-hoc networking support under Android based tablets.

Table 29: Ad-hoc Networking and MANET Reference Documentation Set

Documentation Set	Locations
Further information about OSLRd can be found at the main project site	http://www.olsr.org
Information of support to Android ad-hoc networking. Note that installation of a prebuilt kernel provided by MANET Manager or Cynogenmod version 10.2 or greater integrates ad-hoc into the standard install.	http://www.olsr.org/?q=olsr_on_android
An extensive, but apparently not updated, wireless ad-hoc bibliography	http://w3.antd.nist.gov/wctg/manet/manet_bibliog.html

3.3.2 Radio-based MANET Configuration

An alternative to hosting the MANET on the tablet is to use an external radio that directly supports MANET functionality and that provides an interface for a tablet to act on that MANET. In this approach, the tablet provides the GUI interface and Apps for information and radio management but there is no MANET software on the tablet and the tablet is reduced to an interface-only device, as shown in Figure 15: *A Radio-Based MANET*.

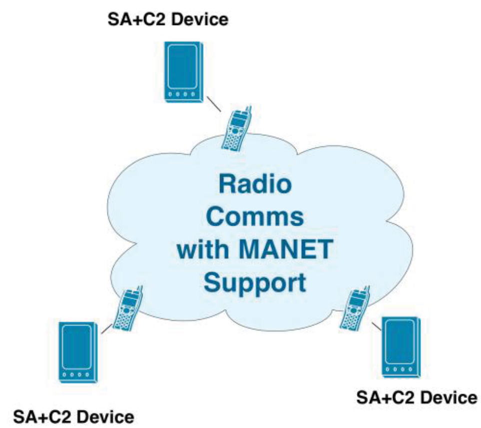

Figure 15: A Radio-Based MANET

Several of the vendors of military grade radios supply products with MANET support, and with interfaces to tablets. Several of these are listed in the previous section on military radios. The two most interesting are the devices from TrellisWare Technologies and Persistent Systems.

3.3.2.1 TrellisWare Technologies

TresllisWare Technologies and their products are outlined in section 3.1.1.1:*TrellisWare Technologies*. Their CheetahNet TW-220, CUB TW-400, and WildCat II TW-130 all have support for MANET and for interfacing with external devices via USB and Ethernet, and the two handhelds support Bluetooth.

They claim the ability to reach 21 kilometers per hop, with 8 hops maximum, for a range of 167 kilometers using their technology. The WildCat product is a dual radio router that can be used for bridging between two different networks supporting the same MANET technology as the handheld radios.

TrellisWare also claims scalability to thousands of units and hundreds of users using Barrage Relay Networks (BRNs) [4]. The key feature of the BRNs technology is the elimination of routing protocols for point-to-point links, and replacing them with a broadcast strategy based on cooperative communications. A technical report on Barrage Relay Networks is available: http://ita.calit2.net/workshop/10/files/paper/paper_1177.pdf

3.3.2.2 Persistent Systems

Persistent Systems is offering a mobile ad-hoc networking solution, called Wave Relay. They claim an improvement over standard mesh networks by continuously adapting to difficult environmental conditions. Their MANET radio products were discussed in section 3.1.1.2:*Persistent Systems*.

Their radio product, the Man Portable Unit GEN4 is a wearable radio that directly supports mobile ad-hoc networking for data, voice, and video. They claim a 3.2 kilometer range for the unit. The have another MANET product, the Quad Radio Router, which is a router with four

separate radios for interconnecting wireless networks, wired network connections, and other connectors.

Wave Relay claims to be a self-forming MANET; however there is no technical information about how their MANET works or the type of routing protocols they are using. During a phone conversation with PS account representatives, it was described as a proprietary MANET solution and, therefore, it is not clear the degree to which PS can inter-operate with industry standard MANET protocols. More information on the algorithms may be available with a signed NDA.

Persistent Systems has several management tools for their MANET products: a Web based tool to configure and manage their products, a visualization tool that integrates with Google Earth and a Management API for third party or customized development and SNMP management tools. Unfortunately the API was not made available during this investigation. Their devices are intended to be complete solutions with limited customization capability available for their customer base.

4 Interpretation of Results

In this section, the radio/handset and tablet hardware products described in the previous section are examined in the context of the architectural options detailed in section 2:*Architectural Specifications*. The intent of this portion of the report is to provide a description and rationale for the most appropriate SA+C2 device solutions to support the DRDC's future initiatives.

4.1 Architectural Options Revisited

Of the six architectural variants presented in section 2, three architectures can be excluded from further examination due to a limited perceived benefit in contrast to the significant drawbacks posed by each approach. The rationale for the decision to exclude those architectures can be seen in Table 2: *Summary of Architectural Approaches* and are summarized below.

- The *Tablet-Only architecture* (architecture 1) suffers from a limited broadcast range and a dependency on closed chipset architectures. Tablet selection dictates which chipset is used and custom software applications may become incompatible should the vendor switch to a different chipset. The chipset interfaces for tablet devices are closed and the architecture and device driver code base is not universally available.
- The *externally assisted tablet architecture* (architecture 2a) using an omnidirectional antenna is not a supported configuration that can be acquired as a COTS solution. The amount of hardware modification to existing tablets outweighs the benefits of a wider broadcast range. Custom hardware modifications, although supported in the community, will violate the product warranty.
- The *wireless router-based externally assisted tablet* (architecture 2b) where a secondary component, a wireless router, is used to achieve a broader broadcast range is deemed to be too complex a configuration for the purposes of this project. The physical hardware setup, the networking configuration and the MANET bridging to achieve a dual network, router-based architecture adds additional parameters to the architecture, making this a higher risk option as compared with other solutions.

What is common about the three architectures referenced above is that the observed benefits from each of these solutions can be achieved by other architectural options without incurring any of the identified disadvantages. These architectural options are, therefore, eclipsed by the remaining architectures and are eliminated from further investigation.

Additionally, a fourth architectural approach (architecture 3b: full spectrum radio) can also be temporarily taken out of contention as a viable solution to form the basis for the SA+C2 device communication capability, although this study will return to this architecture as an enhancement to the baseline capability. For the baseline capability, however, architecture 3b cannot meet the reliable high-throughput communications solution requirements due to technological constraints. As described in section 3, external full spectrum open source software defined radios do not currently provide sufficient support for 802.11 protocols.

While support for 802.11 based IP networking does exist, there are technology limitations that prevent this from being a mainstream solution, most notably:

- The bandwidth limitations restrict data flow to 1Mbps throughput; and
- Processing and computation of signals is limited by the available processing power of the device.

Recent work in FPGA programming may be able to extend this bandwidth limitation, but as of this writing these extensions are not compatible with any known COTS solutions. There is also a technological constraint that moving to the higher bandwidth USB 3.0 interface may increase throughput but introduce interference that will negatively impact the reliability of the device. As a result, the use of SDRs as seen in variant architecture 3b is deemed to be impractical for the hosting of a tablet-based MANET.

It is significant to note that while MANET based SDR communications is not currently a viable architecture, there is still role for SDRs in the SA+C2 device deployment. As discussed later in this section it is possible to combine multiple solution elements to achieve a broader based device environment that provides maximum coverage of the tactical problem space. Section 4.2:*Extending the Capability of the SA+C2 Device* expands on this topic.

This leaves two architectural variants as viable architectural approaches for the SA+C2 device. These options are described below with each architecture shown in context with representational hardware. What is notable about these solutions is that they each represent one side of the hardware/software solution offering space. Specifically, one solution leverages open source community projects hardware and software in its deployment, whereas the other solution is predominantly COTS based.

4.1.1 Option 1: Fully Open Hardware/Software Device Configuration

Within the open source project community, the architectural option that best meets the device based communications needs for creating, using and manipulating MANETs is a tablet device with an external USB Network Adapter. The recommended hardware configuration for this device, as detailed in the table below, includes a TP-LINK TL-WN722N wireless network adapter.

Based on the Tablet with External Wireless 802.11 radio architecture (Architectural Variant 3a), a solution based on this configuration can leverage the openness of the TP link device's design and interface. As previously indicated, this TP network device is the preferred networking component for the developer community due to the openness of its specification and the degree to which the vendor is committed to sharing implementation and coding details with its client base. The TP-Link adapter also has the advantage of accepting alternate and higher gain antennas.

A solution based on the TP-Link network adapter might consist of the elements described in Table 30: *SA+C2 Device using Tablet and External Wi-Fi Radio*; this configuration has already been established and tested and represents one possible configuration for an SA+C2 device and is shown in Figure 16: *Google Nexus 7 and External TP-link Wi-Fi Radio*.

Table 30: SA+C2 Device using Tablet and External Wi-Fi Radio

Hardware	System Software	Applications
A tablet (e.g. Nexus 7) The TP-Link network adapter A OTG cable to connect the two elements.	Linux Cyanogen distribution (nightly build / revision 10.2) Drivers for the TP-link NIC Custom kernel modification to support ad-hoc networking	MANET Manager SA+C2 Applications

The figure below shows these solution elements in their proper configuration: a Nexus 7 tablet connected to a TP-Link TL-WN722N external Wi-Fi radio through an OTG USB cable.

Figure 16: Google Nexus 7 and External TP-link Wi-Fi Radio

4.1.2 Option 2: Device Configuration Based on Commercial Offering

The second viable option for the SA+C2 device is a configuration based on one of the COTS/MOTS MANET capable radios. The recommended technology in this space is the Persistent Systems Man Portable Unit Gen4 combined with the Android Kit to supply connectivity to the handheld graphical device. The PS solution is deemed to be the best suited technology for this class of device deployment due to their frequent firmware updates, which incorporate emerging requirements from military and industry clients, and the availability of their management API.

Persistent Systems, TrellisWare, Motorola and other communications technology vendors have presented a clear message during the course of this study that they are willing to enter into research and directed development projects with DRDC. Given a clearly specified SoW, these vendors would be able to develop a one-off proprietary solution that builds upon their own internal or proprietary technologies. Since the vendors have a greater familiarity with their own interfaces and product architectures, an SA+C2 solution could be developed as a product offering in partnership with DRDC. The vendors would require a certain guarantee with regards to revenue generation and the solution, as a custom product development activity, would be more costly than an in-house research project built on open and freely available tools. Additionally, as a solution built on proprietary technologies, the resulting product would still be a closed architecture and further refinements to the solution would have to be negotiated with the vendor.

4.1.3 Summary of Options

In Table 31: A Comparison of SA+C2 Device Options, the two viable options are evaluated side-by-side in the context of building a suite of tools for mobile SA+C2 devices.

Table 31: A Comparison of SA+C2 Device Options

Criteria	Option 1 Open Architecture Solution	Option 2 COTS/MOTS Solution
Availability	Open architecture system components can be easily acquired and are readily accessible to the open source development community. Provisioning a complete solution for an in-theater deployment would present logistical challenges around form factor and robustness.	The COTS/MOTS equipment can be procured though formal means with full product support. Devices are delivered as complete solutions geared to the military or emergency response environment.
Openness	The solution is fully open with a complete description of architecture, software engineering and interfaces	The solution is partially open. A list of supported protocols is provided and information regarding chipset usage can be obtained. Full disclosure of the architecture cannot be obtained without an NDA or customer agreement.
Modifiability	Source code for all components is available and can be modified without infringing on licensing agreements	Interfaces are protected by IP / NDA agreements and are not modifiable. Altering the operation of the radio would require working with their product team to create a custom firmware deployment. This is not standard practice for small deployments/research organizations.

Criteria	Option 1 Open Architecture Solution	Option 2 COTS/MOTS Solution
Robustness	Suitable for experimentation and lab use, not appropriate for field deployments	Specifically designed (MILSPEC) for in field deployments
Support	Community based support, generally highly responsive with sharing of information and ideas	Commercial support. Limited degree of customization and configuration support
Stability	Individual components QA tested by vendors. Software features from community support generally stable, experimental features less stable.	Only QA products are released ensuring a high degree of stability
Vendor lock in	None, individual components can be replaced with equivalent components in the solution.	As integrated solutions, the component cannot be altered except with vendor approved modifications. Vendors can alter components without notice (e.g. switch to a different chipset with a different interface)
Feature roll out	Very fast turnaround of new capabilities based on emerging research.	Slow feature roll out in keeping with the vendor's engineering practices.
Cost	Inexpensive: $500/ unit	Expensive: $5,000/unit

While integrated COTS/MOTS solutions are more in line with traditional DND procurement practices, it is significant to note that the hardware and software provided through the open source community is more accessible to the general public. The recent trend towards the asymmetric threat (e.g., IEDs) demonstrates that there is tremendous value in knowing the capabilities of devices that can be easily procured and built using ubiquitously available technical information. With the goal of creating new OTM applications, DND benefits from knowing the kind of threat that could be posed by the malicious participants in the developer community [5].

It is also significant to note the difference in cost between the two options: it is possible to provision a complete development lab with multiple tablets, multiple radios, different varieties of full spectrum radios and set of sensor data collection development tools for the cost of two COTS/MOTS based handsets.

Ultimately, to develop proof-of-concepts of new OTM applications leveraging customizations to the device hardware and software, the accessibility of solutions that are based on open source technology wins the day.

As a final note, it is possible to envisage a dual development model that builds on the strengths of both options:

1. Research and development, based on radio security intelligence and in-theater military requirements, can be performed on open source-based lab equipment to create demonstrations of new capabilities.

2. These SA and C2 applications can then subsequently serve as a demonstration of capability that can be shown to the vendor community and help define the next set of features to be integrated into future vendor product releases.

In this way, the DRDC lab can support the rapid development, experimentation and knowledge acquisition process and the vendor is then able to take the clearly defined requirement to create the fully engineered, robust solution as a supported device. The remainder of this report assumes that the first option (tablet with external open source Wi-Fi radio) is to form the basis for the SA+C2 device configuration.

4.2 Extending the Capability of the SA+C2 Device

As described previously in this section, using SDRs to supply the communications and connectivity for a MANET is not currently a viable architecture for connecting SA+C2 devices in a self-contained IP based network. Nevertheless, there is still role for SDRs in the SA+C2 device deployment. As will be shown, it is possible to combine multiple solution elements beyond the deployment of MANET-capable devices and MANET-based applications to achieve a broader based capability that provides a more complete solution for the tactical problem space.

The projects defined in section 3.1.4:*Open Source SDR Support*, most notably the GNURadio open source software project and community oriented hardware projects like HackRF and bladeRF, support a platform for performing sensor data collection activities across a broad radio spectrum. .

The basic SA+C2 device, which includes the SA and C2 applications that are enhanced by access to low-level device, driver and firmware updates to the device components could be further enhanced by including:

- The option of attaching a full spectrum community supported radio; and
- Software to leverage that full spectrum radio to perform sensor data collection activities.

In this way, a dismounted soldier will use the open source Wi-Fi radio to connect to the MANET and receive situational awareness and command directives from the members of the dismounted team or central authority. Those directives may include instructions to enable the device's full spectrum radio to collect sensor data.

The following diagram, Figure 17: *Heterogeneous SA+C2 Device Deployments*, shows the SA+C2 devices in a deployment configuration. When seen in the context of supporting expanded capabilities, several different device variations can co-exist in the ad-hoc network at the same time. In such a heterogeneous device deployment, specific devices can be assigned to users to best meet their tactical role requirement. The diagram illustrates a scenario where three different types of devices are present in an ad-hoc network.

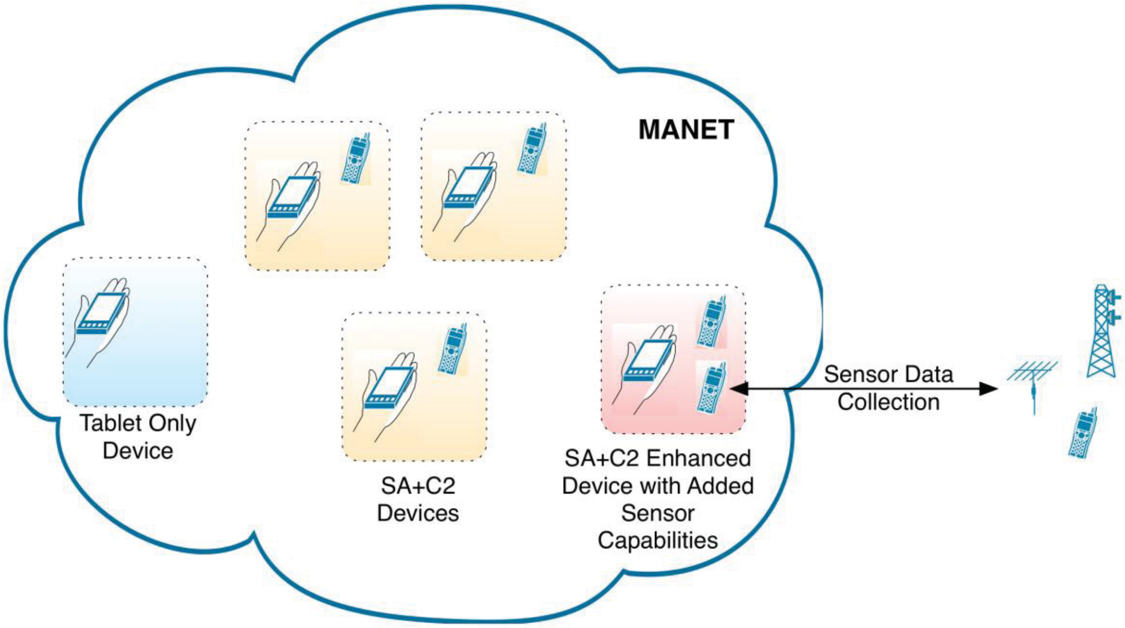

Figure 17: Heterogeneous SA+C2 Device Deployments

- Baseline Tablets (blue): Nodes that have simple requirements for ad-hoc connectivity and access to standard networking applications (e.g., messaging) can use an unmodified tablet device.
- SA+C2 Devices (yellow): Nodes that need advanced networking capabilities, including custom applications that can access and modify local networking protocols and device behavior are supplied with the SA+C2 device, consisting of: open architecture based tablet and external radio.
- Enhanced SA+C2 Devices (red): Nodes with the need to not only participate in the MANET and leverage the custom application but also the ability to perform sophisticated signaling and broad spectrum sensor collection techniques.

It is significant to note that by having the standard SA+C2 device and the enhanced SA+C2 device as separate deployment configurations, the engineering teams that develop and maintain the SA+C2 applications can be kept isolated from the team that develops the capabilities for full spectrum analysis. By compartmentalizing the development efforts, a greater degree of confidentiality can be achieved to minimize the need to disclose architectural details and sensor data collection techniques. One commonly used OS security architecture technique for isolating code execution on devices is presented in the next section.

4.2.1 Co-Existence and Isolation of Code on Android Devices

The ability to segregate operational code into isolated processing spaces is common when deploying security-oriented systems or devices. One such technique, “software jails”, could be applied to the SA+C2 device to isolate tactical software tools for the full spectrum radio from the underlying SA+C2 device hardware. In other words, a software jail could be used to keep a

degree of separation between the communications MANET and the broad spectrum device operation.

A software jail is created by altering the behaviour of the OS file system though the "change root" command. *chroot* (change root) is a command function on Linux platforms that changes, for the calling process, the root location of the file system of Linux. When a process changes the location of the file system root directory, two things occur for that process:

1. An alternative set of user space programs are now in place for that process;

2. It is (in theory) not possible to exit the software jail and return to the prior set of programs located in the original root location of the file system. The only way to exit the jail is to terminate the process itself.

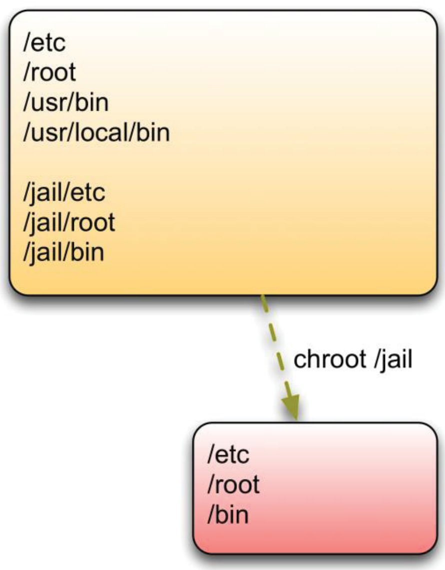

Figure 18: A Software Jail

As an example, the diagram on the left shows a process' view of a file system before and after entering a software jail. Initially, the process is able to access the full base operating system file system which includes full directory set and a directory designated for the jail which includes all the software that will be present for processes that are placed in the jail.

The process executes the command to enter the jail: "chroot /jail".

Once jailed, the process' view of the file system is altered to only see the contents of the jail. In other words, the /jail directory has become the new root location of the file system. The process cannot leave the jail since it has lost reference to any file system elements that for it are placed above its own root location. A jail must contain all software elements (binaries, libraries) that the process needs to fulfil its function since only the elements in the jail are available to that process.

By having processes placed within a software jail, it is possible for an Android device to run code from a different Linux distribution [6].

There are certain limitations to this configuration; specifically, the jailed process using an alternate distribution file system will not be able to use tools that refer to devices or capabilities that are not present on the device. For example, the jailed process will not be able to run graphical X11 applications on the Android display since the X Windowing service is not available on the device. In such cases, graphics-based applications would either have to be used remotely or by developing Android Apps as wrappers for the Linux applications.

4.2.2 Security Enhanced Android

A more advanced and comprehensive method for security the SA+C2 device against compromise is to base the device OS on an Android derivative that is based on Security Enhanced Linux (SELinux). SEAndroid is an initiative out of the NSA to address the increasing use of mobile devices throughout government bodies, along with a perceived need for improved security [7]. Similar to the assessment of this study, Android was chosen as the base platform on which the secure extensions were applied due to the openness of the architecture and availability of code.

As with SELinux, SEAndroid is a series of extension to the operating system code base to add several additional layers of protection in the following areas of OS behaviour:

Greater granularity on access control: A system security policy dictates what operations, tools, and resources are accessible to users, processes or system accounts. This limits the freedom of control individuals (or malicious or compromised processes) have over the system and contains the impact of security breaches.

Sandboxing: Applications and processes execute in isolates spaces that prevent them from being used as a launching pad for system intrusion.

Protection of Android OS element: When porting SELinux to Android, extensions for specific Android architectural components were included in the security architecture including: security labels for the Android file systems (yaffs2), kernel permission checks on the Android IPC mechanisms (Binder IPC) and user space permission checks controlling use of the Zygote commands for operations on objects such as sockets.

While version 4.3 was the first Android release to fully include and enable the SELinux support, version 4.4 is the first release to put SELinux into enforcing mode, where it protects a set of root daemons. Further information regarding Android SELinux support is available at https://source.android.com/devices/tech/security/se-linux.html.

5 Summary and Recommendations

This study has documented six potential SA+C2 device architectures based on MOTS, COTS and open source technologies. These architectures are primarily differentiated by the component that serves as the radio transmission device and the component that establishes the connection to the MANET. These architectures are defined as follows.

1. A tablet-based device where the integrated tablet radio is used to connect to the MANET though software resident on the tablet itself.

2. An assisted architecture where the tablet-based radio broadcast range is enhanced with an external antenna.

3. An assisted architecture where the tablet-based radio's capabilities are enhanced with an external wireless router.

4. An external radio architecture where the tablet leverages an external 802.11 radio while the tablet retains responsibility for participation in the MANET.

5. An external radio architecture where the tablet leverages an external full spectrum radio while the tablet retains responsibility for participation in the MANET.

6. A MOTS/COTS solution where a commercial radio product establishes and maintains the MANET and the graphical component accesses the MANET via the radio.

This investigation has made the following observations about the state of commercial and open source-based radio technologies.

- Programmable interfaces for most COTS/MOTS solutions do exist but are generally not made publicly available to the community. Vendors restrict access to these interfaces to their development team and solution partners. These interfaces may be shared to a wider community but only through a formalized relationship, such as a NDA.
- Conversely, the open source community is actively (and increasingly) involved in the creation of radio-based technologies. It is possible to obtain source code, architectural specifications and device drivers for radio products and extend the capabilities of those products through code modifications.
- Per unit cost differential between COTS/MOTS integrated solutions and the equivalent device created through commercial components is an order of magnitude higher. In a development lab context, a $5,000 military grade radio can be replaced with a $500 open source equivalent.
- Emerging capabilities for radio based devices are quickly released though the open source community although the degree of technical support is less formalized and requires in-depth knowledge on the part of the solution development team.
- Low cost, fully functional broad spectrum radios are becoming easily obtainable through online sources. These tools are of great interest to the radio hobbyist community and it is in the best interest of DRDC to examine the potential threats posed by these new devices.

- Full spectrum radios using low power components are not capable of processing 802.11 protocols at speed and are therefore not capable of serving as the networking device that will connect to the MANET.

Given a goal of developing new OTM applications leveraging customizations to the device hardware and software, the accessibility of solutions that are based on open source technology is most in accord with the project's needs. It is possible to combine multiple solution elements beyond the deployment of MANET-capable devices and MANET-based applications to achieve a broader based SA+C2 device capability that provides a more complete solution for the tactical problem space. The basic device which includes SA and C2 applications that are enhanced by access to low-level device, driver and firmware updates to the device components could be further enhanced by including a full spectrum radio and software to perform sensor data collection activities.

In this way, a dismounted soldier will use the open source Wi-Fi radio to connect to the MANET and receive situational awareness and command directives from the members of the dismounted team or central authority. Those directives may include instructions to enable the device's full spectrum radio to collect sensor information.

Figure 19: *The Proposed SA+C2 Logical Architecture* shows the hardware and software elements that would be required to configure and deploy an enhanced SA+C2 device.

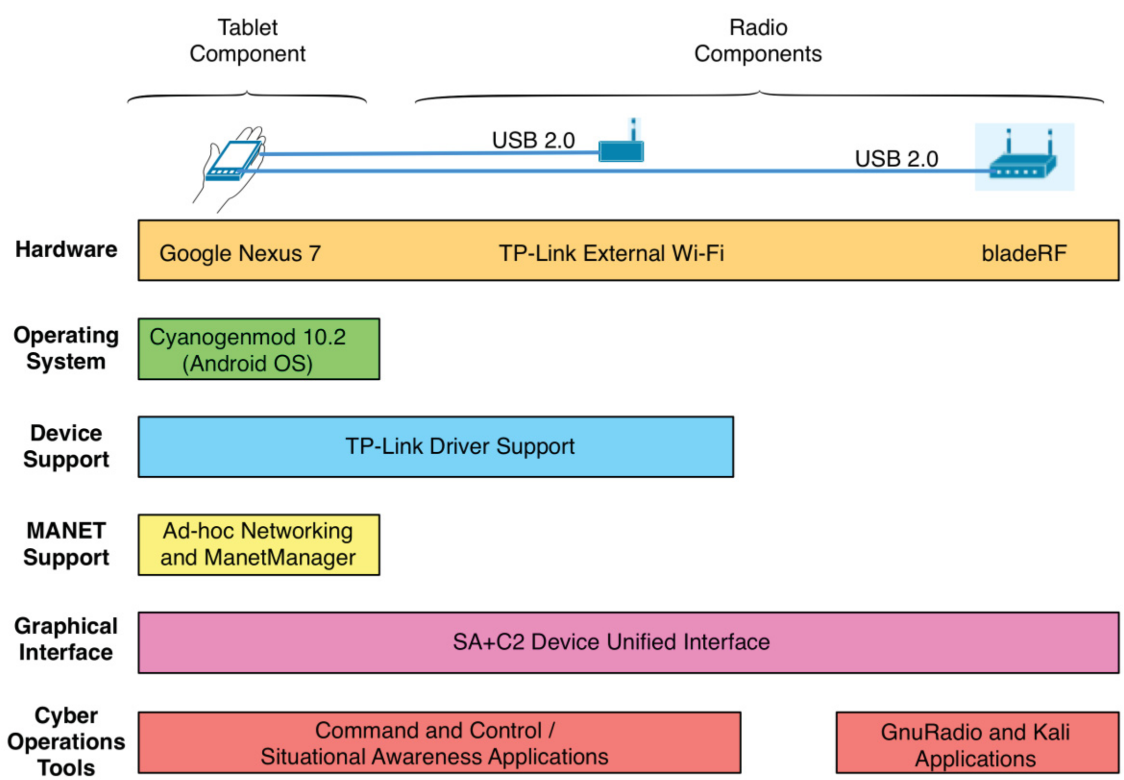

Figure 19: The Proposed SA+C2 Logical Architecture

5.1 Future Work

Based on the results of this study, it is recommended that the investigation into an SA+C2 device be continued to further extend knowledge of the proposed platform. The following areas are recommended for continued investigation:

1. Evaluate existing COTS/MOTS software and hardware platforms on which a research lab could be based.

2. Perform a detailed options analysis for the specific hardware/software selection that will be used to construct and manage a high-bandwidth MANET for dismounted soldiers based on the recommended architecture in this report.

3. Deliver a functioning mobile ad-hoc network solution that supports multi-hop routing and self-configuration to support DRDC's ongoing work in this area.

4. Develop applications for the display device that utilize the MANET as a communications medium.

References

[1] Bowman, E., and S. Kirin. 2006. *The impact of unmanned systems on platoon leader situation aware- ness*. Proceedings of the 2006 Command and Control Research Technology Symposium, June 20–22, 2006, San Diego, CA. Washington, D.C.: CCRP.

[2] Ghosekar, Katkar, Ghorpade. 2010. *Mobile Ad Hoc Networking: Imperatives and Challenges*. International Journal of Computer Applications, Special Issue on Mobile Ad-hoc Networks, 2010

[3] P. du Plessis. 2013. Electronic-Warfare Training Using Low-Cost Software-Defined Radio Platforms. Defense Operational Applications Symposium (SIGE), Sao Jose dos Campos, Brazil 24-27 September 2013, pp. 119-123.

[4] Halford, Chugg, "Barrage relay networks," UCSD Information Theory and Applications Workshop (invited), La Jolla, CA, February, 2010.

[5] Seeber, "Hacking the Wireless World with SDR", Ruxcon 2011.

[6] Gentil, "How to run Ubuntu, ChromiumOS, Android at the Same Time on an Embedded Device", Embedded Linux Conference April 2011

[7] Smalley, Craig. *Security Enhanced (SE) Android: Bringing Flexible MAC to Android*, 20th Annual Network and Distributed System Security Symposium (NDSS '13), Feb 2013

List of symbols/abbreviations/acronyms/initialisms

API	Application Programming Interface
BNC	Bayonet Neill-Concelman
C2	Command and Control
CAF	Canadian Armed Forces
COSW	Cyber Operations and Signals Warfare
CoT	Cursor on Target
COTS	Commercial Off the Shelf
DDK	Device Driver Kit
DND	Department of National Defence
DRDC	Defence Research and Development Canada
EDACS	Enhanced Digital Access Communication System
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
GPIO	General Purpose Input Output
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
IED	Improvised Explosive Device
IP	Intellectual Property
JTAG	Joint Test Action Group
MANET	Mobile Ad-hoc Network
MIMO	Multiple Input / Multiple Output
MOTS	Military Off the Shelf
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSI	Open Systems Interconnection
OSLR	Optimized Link State Routing
OTG	On the Go
OTM	On The Move
PoE	Power over Ethernet
PRR	Personal Role Radio
QOS	Quality of Service
RC	Remote Control
RF	Radio Frequency
RNDIS	Remote Network Driver Interface Specification
SA	Situational Awareness
SA+C2	Situational Awareness and Command and Control
SDK	Software Development Kit
SDR	Software Defined Radio
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SoC	System on Chip
SSR	Soldier System Radio
TCP	Transmission Control Protocol
TTP	"Tactics, Techniques and Procedures"
UHD	USRP Hardware Driver

US-ARL	United States Army Research Laboratory
USB	Universal Serial Bus
USRP	Universal Software Radio Peripheral
VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuit
WISP	Wireless Internet Service Provider
XML	Extensible Markup Language